Security Regulation, Conformity Assessment & Certification

Final Report – Volume I: Main Report

Client: European Commission DG Enterprise and Industry

Brussels, October 2011

Security Regulation, Conformity Assessment & Certification

Final Report – Volume I: Main Report

Client: European Commission, DG Enterprise & Industry

Brussels, October 2011

ECORYS

About Ecorys

At Ecorys we aim to deliver real benefit to society through the work we do. We offer research, consultancy and project management, specialising in economic, social and spatial development. Focusing on complex market, policy and management issues we provide our clients in the public, private and not-for-profit sectors worldwide with a unique perspective and high-value solutions. Ecorys' remarkable history spans more than 80 years. Our expertise covers economy and competitiveness; regions, cities and real estate; energy and water; transport and mobility; social policy, education, health and governance. We value our independence, integrity and partnerships. Our staff are dedicated experts from academia and consultancy, who share best practices both within our company and with our partners internationally.

Ecorys Netherlands has an active CSR policy and is ISO14001 certified (the internationally recognized quality standard for environmental management systems). Our sustainability goals translate into our company policy and practical measures, such as printing our documents on FSC certified paper and compensating our carbon footprint.

ECORYS Nederland BV
Watermanweg 44
3067 GG Rotterdam

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com
Registration no. 24316726

W www.ecorys.nl

Ecorys Labour & Social Policy
T +31 (0)10 453 88 05
F +31 (0)10 453 88 34

Table of contents

List of Acronyms

A2P	CNPP Certification Mark (FR)
AAS	Amsterdam Airport Schiphol (NL)
AC	Access Control
ACBX	Advanced Cabin Baggage X-Ray
ACN	Association of the Air Cargo Industry in the Netherlands (NL)
ACN	Alliance for Digital Trust (FR)
ACPO	Association of Chief Police Officers (UK)
ACS	Approved Contractor Scheme (UK)
ADABTS	Automatic Detection of Abnormal Behaviour and Threats in Crowded Spaces (Project)
ADS	Aerospace, Defence, Security and Space industries Association (UK)
AFNOR	French Association for Standardisation (FR)
AFRP	Armed Forces of the Republic of Poland (PL)
AIA	Aerospace Industries Association (US)
AIS	Advanced Information System
AIT	Advanced Imaging Technology
ANCI	National Association of Italian Municipalities (IT)
ANCISS	Association for Security/Safety and Building Automation (IT)
ANR	National Research Agency (FR)
ANS	National Authority for Security (IT)
ANS	American National Standard (US)
ANSI	American National Standards Institute (US)
ANSSI	French Network and Information Security Agency (FR)
AOE	Authorised Economic Operator
APDCM	Data protection agency for Madrid (ES)
API	Advanced Passenger Information
API	American Petroleum Institute (US)
ASAE	American Society of Automotive Engineers (US)
ASD	Aerospace and Defence industries Association of Europe
ASP	Airport Security Plan
ATC	Air Traffic Control
ATEX	Equipment destined for use in an Explosive Atmosphere (FR)
ATM	Automated Teller Machine
ATM	Air Traffic Management
AVCP	Authority for the Supervision of Public Contracts for works, services and supplies (IT)
AVSEC	Aviation Security
BDS	Body-worn-threat Detection Systems
BIS	Department for Business, Innovation and Skills (UK)
BMBF	German Federal Ministry for Research and Education (DE)
BMWi	German Federal Ministry of the Economy (DE)
BNP	National Proof House for Small Firearms (IT)
BPOL	German Federal Police (DE)
BPVS	Schiphol Security and Public Safety Platform (NL)
BS	British Standard (UK)
BSFSSR	Border Service of the Federal Security Service of the Russian Federation

F	
BSI	British Standards Institute (UK)
BSIA	British Security Industry Association (UK)
BSRBCC	Baltic Sea Region Border Control Co-operation Conference
BTP	British Transport Police (UK)
CA	Conformity Assessment
CAA	Civil Aviation Authority (UK)
CAB	Conformity Assessment Body
CAB	County Administrative Board (SE)
CAC	Conformity Assessment and Certification
CANSO	Civil Air Navigation Services Organisation
CAST	Centre for Applied Science and Technology (UK)
CBP	Customs and Border Protection (US)
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CCTV	Closed Circuit Television
CDSN	Council for Defence and National Security (FR)
CE mark	Conformity mark for products placed on the market in the European Economic Area
CEA	European Insurance and Reinsurance Federation
CEM	Common Methodology for Information Technology Security Evaluation
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CEP	Common Evaluation Process
CertAlarm	Certification Scheme for compliance with EU standards for fire and security products, systems, Installation and services
CESTI	Evaluation Centre for Information Technology Security (FR)
CFE	Conventional Armed Forces in Europe
CI	Critical Infrastructure
CIA	Central Intelligence Agency (US)
CISA	Intra-ministry Committee for the Security of Air Transport and Airports (IT)
CLSPD	Local Council of Security and Prevention of Delinquency (FR)
CNBOP	Research and Development Centre for Fire Protection (PL)
CNIL	National Commission for Information Technology and Liberties (FR)
CNOSP	National Committee for Public Order and Security (IT)
CNPP	National Centre for Prevention and Protection (FR)
COFRAC	French National Accreditation Body (FR)
COPRA	Comprehensive European Approach to the Protection of Civil Aviation
CPD	Construction Products Directive
CPIU	Consumer and Public Interest Unit (UK)
CPNI	Centre for the Protection of National Infrastructure (UK)
CPOSP	Provincial Committees for Public Order and Security (IT)
CREATIF	Network of Testing Facilities for CBRNE detection equipment (Project)
CSA	Committee for Airport Security (IT)

CSI	Container Security Initiative
CSOSG	Concepts, Systems and Tools for Global Security (FR)
CSPN	First level Security Certification (FR)
CTM	Common Testing Methodologies
C-TPAT	Customs Trade Partnership Against Terrorism
CTT	Certification, Testing and Trialling
DA	Designated Authority
DECC	Department of Energy and Climate Change (UK)
DfT	Department for Transport (UK)
DG	Directorate General
DG ENTR	European Commission Directorate General for Enterprise and Industry
DG HOME	European Commission Directorate General for Home Affairs
DG INFSO	European Commission Directorate General for Information Society and Media
DG MOVE	European Commission Directorate General for Mobility and Transport
DGA	Ministry of Defence (FR)
DGAC	General Directorate of Civil Aviation (FR)
DGGN	General Directorate of the National Gendarmerie (FR)
DGITM	General Directorate for Infrastructure, Transport and the Sea (FR)
DGPN	General Directorate of the National Police (FR)
DHS	Department of Homeland Security (US)
Digit-PA	National Organisation for the Scanning of Public Administrations (IT)
DIN	German Institute for Standardisation (DE)
DIS	Defence Industry Strategy (NL)
DKE	German Commission for Electronics and Information Technology (DE)
DLR	Docklands Light Railway (UK)
DNA	Deoxyribonucleic acid
DNS	National Security Directive (FR)
DOJ	Department of Justice (US)
DPA	Data Protection Authority
DST	Directorate of Transport Services (FR)
DTED	Developmental Testing and Evaluation Designation (US)
EA	European co-operation for Accreditation
EAC	Electronic Access Control
EAL	Evaluation Assurance Level
EASA	European Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
ECAC CEP	European Civil Aviation Conference - Common Evaluation Process
ECHR	European Court of Human Rights
ECI	European Critical Infrastructure
ECJ	European Court of Justice
EDA	European Defence Agency
EDS	Explosives Detection System

EFSG	European Fire & Security Group
EFUS	European Forum for Urban Security
EMSA	European Maritime Safety Agency
EN	European Standard
ENAC	Italian Civil Aviation Authority (IT)
ENAV Spa	Italian Company for Air Navigation Services (IT)
ENSG	Electricity Networks Strategy Group (UK)
EnWG	German Energy Act (DE)
EOS	Operational Security Requirements (FR)
EOS	European Organisation for Security
EPCIP	European Programme for Critical Infrastructure Protection
ERDF	European Regional Development Fund
ESO	European Standards Organisation
ETD	Explosives Trace Detection
ETSI	European Telecommunications Standards Institute
EU	European Union
EUISS	European Union Institute for Security Studies
EurAlarm	Association of European Manufacturers and Installers of Fire and Security Systems
EURODAC	European Database of Fingerprints of Applicants for Asylum and Illegal Immigrants
EuroPriSe	European Privacy Seal
FAA	Federal Aviation Administration (US)
FATF	Financial Action Task Force (PL)
FEM der BPol	Technology Centre for Police Equipment of the Federal Police (DE)
FIEEC	Electric, Electronic and Communication Industry Association (FR)
FIPD	Interdepartmental Fund for Petty Crime Prevention (FR)
FNAEG	Automated National File of Genetic Prints (FR)
FOI	Swedish Defence Research Agency (SE)
Frontex	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GDF	Italian Finance Police (IT)
GDP	Gross Domestic Product
GIFAS	Aeronautics and Space Industry Association (FR)
GIFI	General Inspector of Financial Information (PL)
GIS	Group for Strategic impulse (FR)
GPA	Government Procurement Agreement
GTN	National Working Group (FR)
GUM	Central Office of Measures (PL)
H.R.1 Act	Improving America's Security Act of 2007 (US)
HBS	Hold Baggage Screening
HSC	Health and Safety Commission (UK)
HSE	Health and Safety Executive (UK)
IAEA	International Atomic Energy Agency

IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICPP/ULD	The Independent Centre for Privacy Protection of the state of Schleswig-Holstein(DE)
ICT	Information and Communications Technologies
IDMG	International Maritime Dangerous Goods
IEC	International Electrotechnical Commission
IGC	Key Infrastructure Management System (FR)
ILO	International Labour Organisation
IMO	International Maritime Organisation
IMO	International Maritime Organisation
IMP	Institute of Precision Mechanics (PL)
IP	Internet Protocol
IPSA	International Professional Security Association
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ISPS	International Ship and Port Facility Security
ISSC	International Ship Security Certificate
IT	Information Technology
ITU	International Telecommunication Union
JRC	Joint Research Centre
LAG	Liquids, Aerosols and Gels
LEDS	Liquid Explosives Detection System
LOPPSI	Orientation and Programming Law for Internal Security Performance (FR)
LOPSI	Orientation and Programming Law for Internal Security (FR)
LPCB	Loss Prevention Certification Board (UK)
LPS	Loss Prevention Standard (UK)
LRIT	Long Range Information Tracking
LVF	Swedish Operator of Air Traffic Services (SE)
MDE	Metal Detection Equipment
MEDDTL	Ministry for Ecology, Sustainable Development, Transportation and Housing (FR)
MIoIR	Manchester Institute of Innovation Research (UK)
MLA	Multilateral Agreement
MoI	Ministry of the Interior
MRA	Mutual Recognition Arrangement
MRA-ITSEC	Mutual Recognition Agreement – Information Technology Security Evaluation Certificates
MS	Member State
MSB	Swedish Civil Contingencies Agency (SE)
NAB	National Accreditation Body
NATO	North Atlantic Treaty Organisation
NCB	National Certification Body
NCTb	National Coordinator for Counterterrorism (NL)
NEN	National Standards Institute (NL)
NERC	North American Reliability Company (US)
NF	AFNOR Certification Mark (FR)
NFPA	National Fire Protection Association (US)

NGO	Non-Governmental Organisation
NIA	Airport Inspection Team (IT)
NIDV	Netherlands Industries for Defence and Security (NL)
NIN	National Inspection Team (IT)
NIST	National Institute of Standards and Technology (US)
NLF	New Legislative Framework
NLR	National Aerospace Laboratory (NL)
NRA	National Risk Assessment
NRBC	Chemical, Biological, Radiological, and Nuclear (FR)
NRBC-E	Chemical, Biological, Radiological, Nuclear and Explosive (FR)
NSC	National Security Council (UK)
NSC/CSS	National Security Agency / Central Security Service (US)
NSSF	National Standardisation Strategic Framework (UK)
NTTAA	National Technology Transfer and Advancement Act (US)
ODIHR	Office for Democratic Institutions and Human Rights
OECD	Organisation for Economic Cooperation and Development
OFGEM	Office for Gas and Electricity Markets (UK)
OIC	Office of the Information Commissioner (UK)
OIG	Office of Intelligence and Analysis (US)
OIV	Vitally Important Operator (FR)
OJ	Official Journal of the European Union
OMB	Office of Management and Budget (US)
ONVIF	Open Network Video Interface Forum
ORR	Office of Railway Regulation (UK)
OS	Operating System
OSCE	Organisation for Security and Co-operation in Europe
OSP	Operator Security Plan
PA	Population Alert
PC	Personal Computer
PCA	Polish Centre for Accreditation (PL)
PCBC	Polish Centre for Testing and Certification (PL)
PCBS	Passenger and Cabin Baggage Screening
PFIU	Polish Financial Intelligence Unit (PL)
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PISA	Polish Chamber of Security Alarm Systems (PL)
PKN	Polish Committee for Standards (PL)
PNR	Passenger Name Record
PNS	National Programme for Security (IT)
POLALARM	National Association of Manufacturers, Designers and Installers of Alarm Systems (PL)
PoR	Port of Rotterdam (NL)
PPE	External Protection Plan (FR)
PPE	Personal Protective Equipment
PPL	Polish Airports State Enterprise (PL)
PPP	Particular Protection Plan (FR)
PSI	Proliferation Security Initiative

PSIA	Physical Security Interoperability Alliance
PSO	Operator's Security Plan (FR)
PSO	Public Service Obligation
PTE	Passenger Transport Executive (UK)
PZU SA	Polish Insurance Company PZU (PL)
QATT	Qualified Anti-Terrorism Technology (US)
RAG	Risk Advisory Group (UK)
RATP	Autonomous Transport Operator for Paris (FR)
REST	Remote Explosive Scent Tracing
RFF	French Railway Network Operator (FR)
RGS	General Security Reference (FR)
RGS	Railway Group Standards (UK)
RINA Spa	Italian Naval Register (IT)
RISAS	Railway Industry Supplier Approval Scheme (UK)
RISC	UK Security and Resilience Industry Suppliers' Community (UK)
ROC	Receiver Operating Characteristic curve
ROGS	Railways and Other Guided Transport Systems (Safety) Regulation (UK)
RSSB	Railway Safety and Standards Board (UK)
RTD	Research and Technology Development
S&D	Security and Defence
SACS	Swedish Association of Civil Security (SE)
SAFETY Act	Support Anti-terrorism by Fostering Effective Technologies Act (US)
SAGMas	Stakeholder Advisory Group on Maritime Security (NL)
SAIV	Sectors of Activity of Vital Importance (FR)
SAR	Search and Rescue
SARP	Standards and Recommended Practices
SBSC	Swedish Organisation for Certifying Fire Protection and Crime Prevention (SE)
SCADA	Supervisory Control and Data Acquisition
SCB	Sector Certification Body
SDO	Standards Developing Organisations (US)
SDSR	Strategic Defence and Security Review (UK)
SEAP	Security Equipment Assessment Panel (UK)
SEG	Security Executive Group (UK)
SEMA	Swedish Emergency Management Agency (SE)
SGCI	Secretariat General of the Inter-ministerial Committee for Questions on European Economic Co-operation (FR)
SGDN	General Secretariat for National Defence (FR)
SGDSN	General Secretariat for Defence and National Security (FR)
SHEQ	Safety, Health, Environment and Quality
SIA	Security Industry Authority (UK)
SIS	Schengen Information System
SJ	Swedish Operator of Railway Services (SE)
SL	Greater Stockholm Public Transit (SE)
SME	Small and Medium Sized Enterprises
SNCF	French National Railway Company (FR)
SOA	Company Certification Organisation (IT)

SOFF	Swedish Security and Defence Industry Association (SE)
SOG-IS	Senior Officials Group Information Systems Security
SOLAS	Safety of Life at Sea Convention
SoS	Systems of Systems
SS	Security Scanner
STAC	Civil Aviation Technical Centre (French Civil Aviation Authority) (FR)
STIF	Transport Authority of Ile-de-France Region (FR)
SUV	Sports Utility Vehicle
Swelarm	Swedish Trade Association for Companies in Technical Security (SE)
SWIN	Intrusion and Attack Signalization System (PL)
TEC	Treaty establishing the European Community
TECHOM	Technical Protection of Property Development Company (PL)
TEU	Twenty Foot Equivalent Unit
TFEU	Treaty on the Functioning of the European Union
TIP	Threat Image Projection
TLN	Transport and Logistics Netherlands (NL)
TNO	Netherlands Organisation for Applied Scientific Research (NL)
TOE	Target of Evaluation
TRANSEC	Transport Security and Civil Contingencies Directorate (UK)
TRIS	Technical Regulations Information System
TSA	Transportation Security Administration (US)
TSF	Taking Standardisation Forward Committee (UK)
TSFS	Swedish Transport Agency's Statute Book (SE)
TTF	Technical Task Force
UDT	Technical Inspection Centre (PL)
UKAS	United Kingdom Accreditation Service (UK)
UN	United Nations
UVDB	Utilities Vendor Database (UK)
VDE	Association for Electrical, Electronic & Information Technologies (DE)
VDE	Vapour Detection Equipment
VDE FNN	VDE Forum Grid Technology/Grid Operation (DE)
VdS	VdS Schadenverhütung GmbH (Testing Institution for Fire Protection and Security) (DE)
VIS	Visa Information System
WCO	World Customs Organisation
WMD	Weapons of Mass Destruction
WTMD	Walk Through Metal Detector
WTO	World Trade Organisation
XP-DITE	Accelerated Checkpoint Design Integration Test and Evaluation (Project)
ZVEI	German Electrical and Electronics Industry Association (DE)

Preface

This document constitutes the Final Report for the “Study on the regulatory framework and certification / conformity assessment procedures in the security sector” undertaken in the context of the Framework Contract on Security (ENTR/09/050) between the European Commission, DG Enterprise and a consortium led by Ecorys Nederland BV.

The main elements of this Report concern the overview of the EU regulatory environment, together with an assessment of the environment for conformity assessment and certification of security products. National surveys of the security regulatory environment and conformity assessment and certification environment for 7 EU Member States are provided in an accompanying report (Volume II: National Surveys). Drawing on the findings from the EU and national surveys, this Report identifies and assesses potential EU-level policy options to enhance conformity assessment and certification of security products.

The organisations that have contributed to this report are:

- Ecorys;
- DECISION Consulting;
- TNO;
- MIoIR (Manchester Institute of Innovation Research);
- FOI (Swedish Defence Research Agency).

The individual contributors to the study (including the national surveys) are as follows:

- Robert Piers, Jolanta Rekiel, Douwe Wielenga, John Edwards, Ignacio Gomez (Ecorys);
- Sébastien Rospide, Gerard Briard, and Thibault Montoroi (DECISION Consulting);
- Marieke Klaver, Imelda van de Voorde (TNO);
- Thomas Teichler, Abdullah Gok, Andrew James (MIoIR);
- Anders Eriksson (FOI);
- Roger Warwick (Independent consultant / Pyramid International);
- Sandra Mezzadri (Independent consultant).

Team Leader and Coordinator:

- Paul Baker (Ecorys Associate Consultant).

Executive Summary

Introduction

This Report describes the findings from the study on “Security Regulation, Conformity Assessment and Certification”, which is the first study undertaken in the context of the Framework Contract on Security (ENTR/09/050) between the European Commission, DG Enterprise and a consortium led by Ecorys Nederland BV. The main elements of the study are as follows:

- **General Framework:** providing a general conceptual framework linking the regulatory environment to conformity assessment and certification of security products;
- **Regulatory Snapshot:** providing an overview of selected elements of the regulatory framework applying to the security sector at national and EU level with a focus on regulations applying to security products;
- **Analysis of Conformity Assessment and Certification procedures:** identifying and analysing the rules and regulations applying to conformity assessment and certification procedures for security products at national and EU level;
- **Options for enhancing Conformity Assessment and Certification procedures:** identifying and assessing possible EU-level options for enhancing conformity assessment and certification procedures.

The analysis of the overall EU situation (as documented in the Main Report) has been supported through national surveys conducted for 7 Member States (Germany, France, United Kingdom, Italy, Netherlands, Poland, Sweden), which are documented in Volume II of this report.

Background and general context

The focus of the study is on two main areas of the general environment (framework conditions) of the security sector, namely the regulatory environment and the environment for conformity assessment and certification in the EU. These two areas have been highlighted as of importance for future European security and where EU-level action may be warranted. This is the case, for example, in the Commission’s Communication on "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations" (COM(2009) 691 final). Both a more harmonised regulatory framework and an improved infrastructure for validating and certifying security products and technologies would provide mechanisms that contribute to enhancing security within the EU and have the potential to enhance the competitiveness of the EU security industry, particularly by reducing the current fragmentation of EU markets.

Taking a broad perspective, the highly fragmented nature of the European market has been identified as one of the most significant factors hampering the development of the security industry within the EU. This market fragmentation contributes to higher costs for European industry and, in turn, procurers and users of security products. It is also part and parcel of a business environment in the EU that some stakeholders argue is unattractive for the future development and long term competitiveness of the security industry. From the standpoint of industrial policy, this situation raises important considerations for future growth and employment prospects in a sector associated with a high potential for technology development and innovation. From a security and societal standpoint, weakening of Europe’s position in terms of access to and control over technological

developments in the security field can have important implications for Europe's future capabilities and independence to provide security solutions that correspond to the needs of its public authorities, businesses and citizens.

Overview of the regulatory environment for security products

With regard to the regulatory framework, we concentrate mainly on the linkages between regulatory frameworks and other rules relevant to security products and their implications for conformity assessment and certification requirements and procedures. It is evident, however, that this represents only a small part of the overall regulatory environment relevant to the security sector .There remain many areas where in-depth analysis may be warranted.

In attempting to provide an overall assessment of the regulatory framework applying to the security sector at national and EU level and, specifically, regulations applying to security products a number of important features need to be borne in mind:

- At EU-level there is **no common (single) framework that applies to security products and the market for security products** as a whole. Rather, there are a multitude of different rules and regulations that have been adopted to cover security concerns related to different sectors and activities, and with different purposes:
  - They may directly reflect overarching security requirements; for example, common minimum security levels for airports and ports, or biometric passport requirements to improve identification of persons;
  - They may concern the interface between security and individual rights and privacy; for example data protection rules regarding the processing and movement of personal data;
  - They may be motivated by (internal) market and competition considerations; for example public procurement regulations;
  - The may relate to 'generic' product requirements (e.g. health and safety).
- EU-level and national **legislation in the area of security is relatively recent** and mainly threat driven. It follows specific events rather than long term risk / threat assessment and planning;
- EU-level **legislation is limited in scale and scope:** relatively few binding legislative acts have direct implications for the security sector and the supply of and market for security products. In general, EU legal instruments contain rather generic provisions that set minimum common requirements for security procedures and only occasionally apply directly to security products;
- **Member States retain a degree of flexibility** in transposing EU Directives into national law, leaving room for interpretation. Further, national governments typically retain the prerogative to impose more stringent security requirements. Thus, national differences in rules and regulations, which may be well justified on individual country's security threat assessment, can and do contribute to market fragmentation.

Overview of the conformity assessment and certification (CAC) environment for security products

With regard to existing CAC frameworks, two main areas of concern have been identified:

- **Absence of common certification systems** for security products at a European level and no mechanism of mutual recognition across countries of products certified at a national level;
- **Slow speed of response and adaptation of certification procedures** notably where new security threats require the implementation of new security solutions and technologies.

In general, such concerns point to the potential for EU-wide policy initiatives to improve conformity assessment, testing and certification of security products, by enhancing approvals and certification procedures and infrastructure. A general objective of such initiatives could either be to generate new certification strategies or harmonise existing ones, with the aim of ensuring that CAC frameworks are adequate to meet EU requirements. Moreover, moving to greater mutual recognition between countries, increasing transparency of procedures, and improving the level and quality of interaction between approval and certification bodies could raise the efficiency of the system and support EU security technology development.

EU 'generic' approach under the New Legislative Framework

The general EU framework for conformity assessment and certification of products is contained within the New Legislative Framework (NLF). To date, the use of the NLF has mainly related to aspects such as protection of health and safety of products but also including electromagnetic compatibility. Some categories of security-relevant products are, however, covered by the Construction Products Directive/Regulation which follows an NLF approach; however this relates to products that are typically somewhat removed from the types of threats normally associated to major civil-security concerns. And at the same time security-related requirements for products are not handled through an NLF approach.

Nonetheless, in principle at least, the NLF could form the basis for any future regulatory approach and to set *inter alia* performance requirements for security products and technologies.

Supra-national approaches in the security domain

Moving away from 'generic' approaches to conformity assessment and certification, it is important at the outset to note that in most instances current approaches – particularly where they concern supra-national schemes – are relatively new. Accordingly, their lack of maturity makes it difficult to assess their relative strengths or weaknesses. The current situation may be summarised as follows:

- **General / 'Traditional' security equipment.** A limited number of security-related equipment (e.g. fire alarm and fire protection equipment) is covered within the scope of the Construction Product Directive/Regulation and, thus, falls with the provisions for mutual recognition of certificates of compliance with EU regulations. Otherwise, for what may be termed 'traditional' security equipment (e.g. intruder alarms, access control, CCTV surveillance, etc.), the EU market is characterised by national schemes for conformity assessment and certification. Where certification is required – and such requirements are by no means common across Member States – suppliers must usually submit to local conformity assessment and certification procedures. To date, there has been very little progress towards common certification schemes and/or mutual recognition of certificates;
- **Priority / 'New' security equipment.** Regulation of the aviation sector and biometric identification are among the clearest examples where legislation sets (performance) requirements for security products. But, for both areas there is no complete harmonisation of performance requirements across countries and, consequently, there exist differences in national conformity assessment and approval/certification. Also noticeable is the limited scale of the infrastructure for undertaking testing of these categories of security technologies: there are only four test centres in the EU that test and certify biometric equipment; similarly, in the aviation sector, under ECAC CEP there are only 4 test centres for Explosive Detection Systems (EDS) and 3 centres for Liquid Explosive Detection Systems (LEDS). With regard to other sectors covered by the study – maritime/ports, urban transport, and other critical infrastructure (e.g. power generation, transmission and diffusion) – most supra-national regulations are pitched in terms of requirements for overall security procedures and processes. Typically, such regulations do not set out performance or technical requirements for security products;

- **IT security and data protection.** The development of common and supra-national approaches to conformity assessment and certification is often a reflection of the presence of a multitude of differing national approaches. For example, the Common Criteria for Information Technology Security Evaluation - Common Criteria (CC) for short - are the outcome of the efforts of a number of governments to develop harmonised security criteria for IT products. However, the CC are seen by some to be too slow and too bureaucratic to respond to rapidly changing developments in information security technologies; in part because of they rely on consensus for the development of new standards. It appears that there is some slippage in the use of CC evaluation procedures with certain countries pushing their own national testing regimes.

Insurance-related frameworks for conformity assessment and certification

Moving away from the regulatory environment, the insurance industry has historically had an important influence on the development of conformity assessment and certification requirements for security products. This is most evident for 'traditional' security products for which the insurance industry has fostered the development of standards for safety and security products. This has been accompanied by the development of corresponding conformity assessment and certification procedures. The existing frameworks are essentially nationally organised and with little mutual recognition of certificates between countries. Certifying bodies linked to the insurance sector have been slow to embrace EU-wide solutions, a development that has only started recently.

Key issues relating to the rules, regulations and procedures for conformity assessment and certification of security products

The analysis undertaken by the study has identified a range of issues that seem relevant to identify and assess possible approaches and EU-level options to enhance current CAC procedures:

- **National specificities versus common approaches.** While there may be broad agreement at EU-level on the general nature, scope and perceived magnitude of civil-security threats, when considered from a specific local or sector context these can translate into more heterogeneous security situations and corresponding requirements;
- **Administrative and regulatory responsibilities.** Rules and regulations setting the conditions of supply and utilisation of products in relation to civil security are determined at different administrative levels from supra-national, via national and regional, down to very local levels (e.g. municipal authorities). While it is the case that international (including EU) frameworks for civil security exist in certain sectors (e.g. aviation and maritime), more often t responsibilities for civil security remain at a national-level and are even further devolved to regional and local levels;
- **Market organisation and institutional arrangements.** The security market embraces a range from primarily institutional market segments – reflecting public sector responsibilities for civil security – through to essentially private sector market segments. In the middle of this range is something of a grey area where boundaries between public and private sector responsibilities can be blurred. This creates uncertainty over the allocation of security responsibilities and tensions between those prescribing security requirements and those responsible for implementing security measures;
- **Limited involvement of end users and other stakeholders in the elaboration of standards.** While there is an underlying principle that standards should be developed on a 'consensus' basis, in many areas there appears to be little involvement of end-users. Standardisation bodies, certification bodies, technical experts (that may themselves be part of the CAC infrastructure) and other stakeholders such as the insurance industry tend to comprise the main participants in the development of standards, with lower representation of end-users;

- **Product-based regulation versus obligations and conditions of use for security products.** The regulatory framework relevant for security products can be based on differing approaches:
  - ***Product (supply) based***. Legislation may apply directly to a certain category of security product, setting out 'blanket' conditions (e.g. minimum technical specifications) to which the products must conform in order to be made available on the market;
  - ***Sector (demand) based***. Legislation may apply to the customers and end-users of security products; for example where security requirements are set for specific economic sectors or activities. Such regulations are limited to setting obligations on the relevant 'actors' – either public or private sector, or both – to ensure adequate measures are implemented to maintain security;
  - ***Hybrid 'sector-product' based***. A 'hybrid' of these approaches is provided where legislation not only sets out obligations to fulfil certain security functions but also sets out the relevant means (and technical specifications thereof) through which the security function is to performed.

  To date, the main thrust of security-related regulations has been of the second type listed above. Security regulations are typically orientated towards a particular type of (economic) environment (e.g. aviation, maritime, critical infrastructure, etc.) or activity (e.g. border control, management and transport of hazardous materials, etc.). As such regulations do not directly provide technical specifications for security products, leaving the evaluation of the appropriateness of employed products/technologies to the discretion of the relevant authority or inspectorate.
- **Standards and CAC for single equipment versus systems.** Existing performance standards and corresponding CAC arrangements are at the level of individual equipment and components. Many stakeholders point to the need for systems approaches that look at systems that combine different equipment (e.g. complex checkpoint solutions) and that also take into account the provision of services that are directly linked to products/equipment. Conformity of individual products/equipment does not by itself ensure the effective provision of security;
- **Certification of products versus certification of systems.** Addressing conformity assessment and certification requirements for complex systems raises issues related to which of the parties are positioned to obtain approval/certification. For individual products it is evidently possible for the manufacturer/supplier to obtain approval/certification of their product. However, when dealing with large systems that integrate equipment from different suppliers and/or where the configuration and operational characteristics are specific to the particular environment in which the system is deployed, either the system integrator (where there is one) or the actual operator will need to obtain approval/ certification of the system. In this regard, given that large systems are more closely linked to the environment in which they are deployed, it is probably more difficult to harmonise certification of systems than it is to harmonise certification at the individual product level;
- **Privacy and data protection issues.** The on-going debate over the use of security scanners highlights the role of 'ethical' issues such as privacy and data protection. In the absence of a clear European framework in this area and at national levels also, there is a lack of clear guidelines for equipment/technology providers with respect to accepted and acceptable performance requirements;
- **Certification not appropriate for all conformity assessment issues in the security sector.** Conformity assessment in the security sector is sometimes done on the basis of a classified 'standard'. The classified character of the 'standard' contributes to the security function. In such cases, the integrity of the conformity assessment processes is of critical importance. This may limit the scope for assessments to be conducted by private certifying bodies and call for additional checks on the integrity and reliability of certifying bodies;
- **Confidence in CAC frameworks.** Any efforts towards common EU approaches for CAC must be able to guarantee confidence in the 'quality' and 'independence' of approvals and certification outcomes. In particular, this relies on the strength of mechanisms for accreditation

of conformity assessment bodies and test laboratories (and other similar organisations) responsible for verifying conformity.

Framework for establishing potential EU-level approaches for conformity assessment and certification of security products

Categorisation of security products

In defining possible options for CAC account needs to be taken of the wide diversity in security threats and corresponding capability and performance requirements; in security products and security technologies; and in security markets, both in terms of economic sectors/activities and categories of customers (institutional, private, etc.), as well as in the 'drivers' shaping demand. While interaction of such factors implies a complex set of market conditions, the general situation can be characterised in terms of two contrasting market-product segments that illustrate the differing challenges for any EU initiatives towards conformity assessment and certification:

- **General purpose security products (Type-1):** security products and solutions aimed at addressing 'familiar' security situations (security threats or functions) through the application of improved but existing technology. This includes what may loosely be called 'traditional' security equipment (e.g. intruder detection, CCTV, access control, security barriers);
- **Priority and sensitive security products (Type-2):** security products and solutions addressing 'unfamiliar' or new types of threats that require the development or application of new technologies, and equipment and may be extended to changes in organisation and implementation of security functions; for example through the automation of security functions. This includes what may loosely be called 'new' security equipment (i.e. corresponding to products/technologies developed primarily to address threats as terrorism, organised crime, cyber-crime, etc.).

Main policy challenges by security market-product segment

Using the two market-product segments outlined above the main policy challenges relating to the rules, regulations and processes for conformity assessment and certification may be summarised as follows:

- **For Type-1 products**, the main policy challenges stem from the **absence of common EU-wide certification of products**. Manufacturers and suppliers point the fact that they are faced with *de facto* requirements to separately certify products in almost all EU countries as there is no – or very limited – recognition of certification between countries. As a consequence, manufacturers and suppliers face the administrative burden and cost associated with multiple certifications of their products which, particularly for SMEs, represents a significant barrier to supplying new markets;
- **For Type-2 products**, the range of policy challenges is wider, since there is often a direct link to issues of EU Internal Security, including **ensuring minimum security performance levels** (and promoting higher ones) and **speeding-up the deployment of new technologies and solutions**. Here, a common approach to conformity assessment and certification could contribute to reducing/avoiding the fragmentation of newly emerging market segments in the EU. An EU wide CAC system – based on common performance criteria – should increase market transparency by providing end-users with greater information on the relative attributes of different products and, hence, promote competition.

Characterisation of potential EU-level policy approaches for CAC of security products

Using the two market-product segments outlined above, the main elements and issues to be addressed by possible policy actions to enhance existing frameworks for conformity assessment and certification can be summarised as follows:

- **For Type-1 products**, for which there exist performance and other technical standards – albeit differing at national levels – and national infrastructures for testing equipment in many Member States:
  - **Standards harmonisation:** The first focus for EU policy intervention would relate to the development of harmonised European Standards and the promotion of their use within the market;
  - **Market recognition of European standards:** The second focus for EU policy intervention relates to the extent of market recognition of products certified as conforming to European Standards. The market may recognise European Standards and duly certified products without the need for further EU intervention (i.e. a voluntary solution is achieved) but, if there is continued insistence on national certification, additional EU intervention may be justified to promote recognition of European Standards and EU-wide certification;
  - **Regulation:** A legislative approach may be adopted if a market-based solution resulting in common (EU-wide) certification or mutual recognition does not develop. This could take the form of the introduction of specific legislation for security products following, for example, a NLF approach;
  - **Conformity assessment and certification:** Whether a market-based or legislative approach is adopted, existing accreditation procedures and conformity assessment infrastructures (e.g. testing laboratories) could be used to provide conformity assessment (testing) services and certification in accordance with harmonised European standards.
- **For Type-2 products**, consideration needs to be given both to the process of defining EU standards, including those related to testing methodologies and test criteria, and to the overall design of an EU system for conformity assessment and certification. In this regard a number of issues arise:
  - **Regulation:** As described earlier, relevant EU regulatory frameworks can be characterised as product (supply) based or sector (demand) based, or a hybrid combination. A sector-based approach for CAC would complement existing sector-based regulatory frameworks but would be limited only to the sectors covered by legislation. A product-based approach would provide a general system of approval/certification of categories of products but would need to address possible variations in requirements for different sectors/activities. A product-based or technological-based framework may be preferable, since this would create a single system of CAC for product categories, irrespective of the sector in which they are deployed;
  - **Standards:** A basic principle for CAC is that it should demonstrate conformity to recognised standards (preferably international or European) or other transparent and objective criteria – such as technical regulations – in a non-discriminatory manner. Similarly, when setting performance measurement standards, the measurements or test results should be traceable to recognised (preferably international or European) measurement standards. These conditions pose a number of difficulties with respect to Type-2 products, particularly for new technologies for which recognised standards may not exist and where security performance requirements and associated test criteria can be 'sensitive' (e.g. classified or secret) information;
  - **Accreditation:** A common EU CAC system for security products would have to command the confidence and support of Member States throughout the EU, thus enabling the principle of mutual recognition to be accepted (i.e. Member States recognition of certification received

from another Member State or, possibly, a central EU Certifying Body). To ensure confidence in the CAC system and procedures, adequate and appropriate 'checks and balances' would be required to assure necessary expertise of conformity assessment bodies and to assure that applied conformity procedures are appropriate;

- **Certification:** A fundamental question concerns the extent to which national authorities would be prepared to accept the principle of mutual recognition of approval/certification by another Member States. An alternative may be to adopt a more centralised approach with approval/certification being issued by a single organisation subject to specific scrutiny by the EU with, or on behalf of, national authorities. Nonetheless, for some product categories, Member States may consider that they have an essential obligation to undertake their own national testing and validation of certain categories of security products.

In terms of the institutional structure necessary to support CAC of security products, for Type-1 products it would seem appropriate to build on existing CAC schemes. However, given that Type-2 products are associated with specific regulatory responsibilities (and expertise) and require specialist technical expertise, a dedicated CAC scheme and infrastructure is more likely to be necessary.

Definition of possible EU-level initiatives to enhance conformity assessment and certification of security products

Outline of policy options

To identify and assess the potential impacts of possible EU-level initiatives to enhance conformity assessment and certification of security products, a limited number of policy options have been defined:

- **Option 1 - Baseline.** This scenario represents a continuation of the currently existing situation. Here, no common EU-wide system providing conformity assessment and certification (CAC) of security products would exist. Security products subject to approval/certification requirements would continue to undergo national testing, validation and approval/certification procedures. No priority would be given to certain products. Furthermore, no additional development of EU-level structures and processes for the implementation of conformity assessment and certification requirements and procedures would take place;
- **Option 2 - A step by step approach.** This option would apply to the two market-product segments described above (i.e. Type-1 and Type-2) and would consist of two sub-components:
  - ***Option 2.1*** *- EU CAC for 'general purpose' security products (Type-1).* Intended to cover security products aimed at 'general' security markets and/or based on comparatively mature technologies (Type-1);
  - ***Option 2.2*** *- EU CAC for 'priority and sensitive' security products (Type-2).* Intended to cover security products aimed either at 'specific' markets and/or based on comparatively new or innovative technologies (Type-2);
  - For each product type it is assumed that a step-by-step approach would be adopted under which EU initiatives start with limited product category coverage, to be expanded over time and in response to changes in security-based and market-based priorities. Criteria for the prioritisation of product categories are discussed in the following subsection.
- **Option 3 – An all-encompassing approach.** This would be a situation where an EU-wide CAC system is in place for all security products (both Type-1 and Type-2) all at once.

Prioritisation of security products and technologies to be covered by an EU-level CAC schemes

Policy Option 2, outlined above, assumes a step-by-step approach that incorporates a prioritisation of security products and technologies to be covered by EU-level initiatives for conformity assessment and certification. Accordingly consideration of the possible relevant criteria that may be utilised for prioritising products and technologies is required. In this context, possible criteria may be identified in relation to the main policy challenges (policy areas):

- **EU Internal Security Policy:** from a security perspective the overriding concern is to ensure the rapid and effective deployment of security products/technologies to address the most pressing security threats and challenges;
- **EU Internal Market Policy:** from an internal market perspective the main consideration is to reduce the existing fragmentation of markets within the EU. Accordingly, the main criteria for prioritisation of security products and technologies to be covered by an EU-wide CAC scheme relate to the prevalence and magnitude of barriers to trade and to the extent to which there is a lack of a 'level playing field' within the EU;
- **EU Industrial Policy:** from an industrial policy perspective, two criteria for prioritising products and technologies come to the fore. Firstly, the potential to reduce costs and administrative burden placed on manufacturers/suppliers of security products as a result of existing CAC requirements (e.g. multiple certifications). Second, the potential contribution that an EU-wide scheme could make to enhance the competitiveness of the EU security industry. Concerning this second criterion, two particular elements may be identified: (a) segments where EU industry has a comparatively strong market position and for which a more unified market within the EU could serve to reinforce this position and (b) potential benefits that may come from developing EU-wide CAC schemes that also support technology development and innovation by EU industry.

While opinions among stakeholders differ on the question of which security products and technologies should be prioritised, the following may be proposed:

- **For Type 1 products,** a starting point may be to start with security alarm and hold-up alarm systems (for which there is already a private/industry led scheme; CertAlarm) that may be extended to other categories of security electronics products for which European Standards exist (e.g. sensors, control panels) and towards other forms of perimeter and surveillance equipment (e.g. security CCTV systems);
- **For Type 2 products,** a similar approach of building on existing schemes/procedures would bring in products where EU performance requirements already exist (e.g. airport scanners, biometric identity documents). In the case of scanners, this may be extended towards cargo and container scanners which would be relevant for both the aviation and maritime sectors and would have wider application in terms of supply chain security in general. Another area that has been mentioned is eGate type solutions for border control management, which could also have possible applications beyond the aviation sector. Although there remains some uncertainty as to whether there will be wider deployment of eGate type solutions, a broader based EU CAC scheme could be considered that covers biometric based access control systems employed in a variety of security contexts.

In general, the limited identification of priority products / technologies suggests that there remains a need for greater monitoring of EU markets for security products and of developments in security products and technologies. It may be appropriate therefore for the European Commission to set up or support a monitoring scheme/methodology, which could include also consultation with stakeholders representing both the supply and demand side and authorities with security responsibilities. This could serve to identify those areas where standards and CAC requirements are most pressing.

Identification and assessment of potential impacts of possible EU-level initiatives to enhance conformity assessment and certification of security products

The nature and character of the security sector has proved to be a strong limiting factor for the quantification of potential impacts, and sometimes even in qualification of the analysed policy options. From both the supply-side and demand-side there is hesitancy to provide information that may be deemed sensitive from a security perspective. Furthermore, information may also be commercially sensitive in so far as it relates, for example, to the cost structures of suppliers of security products. It should also be noted that costs associated to conformity assessment procedures (e.g. fees for product testing) are typically negotiated between the product supplier and providers of conformity assessment services. Quantification of potential impacts is further hampered by the absence of available information on the volume of CAC activities currently undertaken within the EU. This being the case, the analysis is restricted mainly to a qualitative assessment of potential impacts.

For the purpose of summarising the potential impacts of EU-level policy initiatives, the following provides a generic description of the main identified impacts – relative to the Baseline Scenario – associated to Option 2 (as outlined above). For Option 3, the impacts should be similar but generally larger in magnitude. However, Option 3 is considered to be considerably less feasible from a technical and political perspective than Option 2.

Impacts on producers

Main impacts for producers from an EU certification scheme (with mutual recognition) are:

- **Reduction of costs associated to multiple testing to obtain national certification.** Security products will have to be certified only once rather than multiple times, thus reducing overall conformity assessment and certification costs;
- **Reduction of adaptation costs to meet national product standards/specifications.** Common EU product standards reduce the need to produce product variants adapted to meet different national standards;
- **Reduction of the need for product trials (for Type-2 products).** The possibility to certify products meeting EU requirements after initial trials should reduce the subsequent need for further national and/or client trials;
- **Reduction of the 'time to market' of products.** Having obtained EU certification, products may be introduced to the whole EU market without delays that are caused now by the need to obtain national certification;
- **Improved alignment of production to the expected EU market as a whole.** Production (of certified products) can be aligned at the outset to the expected size of the EU market rather than being conditioned on the uncertain timing associated with obtaining national certification;
- **Reduction of risk that competitors are able to 'replicate' new product developments and innovations.** Simultaneous access to the EU market as a whole limits the opportunities for competitors to use delays in obtaining national certification to launch competing products;
- **Enhanced transparency of performance requirements and standards / specifications (Type-2 products).** Common EU performance requirements and conformity assessment protocols should enable producers to better develop products according to 'predetermined' criteria, reducing uncertainty of product conformity assessment outcomes;
- **Acceleration of development process (Type-2 products).** A common regulatory framework with reference to defined product standards/specifications should make it easier for producers to direct their RTD efforts to meeting regulatory/market requirements.

Potentially negative impact for producers relates to the additional costs of obtaining EU certification (for products that are currently not covered by national conformity assessment and certification requirements but that will be brought within a future EU-wide system).

Impacts on market conditions

Potentially positive impacts on market conditions are:

- **Increased transparency regarding product performance.** EU certification provides an indicator of product performance based on common standards/specifications and, hence, increases market transparency;
- **Increased market openness.** Increased market transparency should reduce market entry barriers by facilitating market acceptance of (certified) products offered by new market entrants and reducing the importance of ''reputation effects';
- **Increased competition in security product markets.** Greater market transparency and openness should reduce fragmentation and increase the level of competition within markets. Existing suppliers will be more easily able to serve different national markets, which may be particularly beneficial to SMEs. The EU market would also be more attractive to new entrants, both new business start-ups and non-EU based suppliers. Increased competition should put downward pressure on the price of security products, which reduces costs for procurers / users of the products;
- **Increased competitiveness of European manufacturing industry.** Increased competition should drive improvements in productivity performance by forcing improvements in production efficiency and/or raise value added (e.g. higher value-added products). At the same time, improved market access that increases the size of the potential market for new products, should provide a positive incentive for producers to engage in RTD activities and promote innovation. Finally, EU certification may support exports of products to markets outside the EU if it engenders greater recognition in international markets than the existing multitude of national certification schemes.

The main identified potentially negative impact on market conditions concerns the possibility that minimum EU standards may become *de facto* market requirements. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or innovative' products, particularly if they are more costly than standard products that comply with minimum requirements.

Impacts on procurers and users

The main identified potentially positive impacts for procurers and users are:

- **Lower price for security products.** As outlined above, there are a number of impacts that affect producer costs and prices and that should feed through to the purchase cost of security products;
- **Increased product choice / availability.** Increased market openness should result in more suppliers on the market. At the same time, a less fragmented EU market should promote RTD and innovation and raise entry into the market of new technologies and innovative solutions;
- **Enhanced information / transparency on product performance.** An EU-wide conformity assessment and certification scheme should increase market transparency and provide potential purchasers with greater information on product performance. This should contribute to reducing information asymmetries between purchasers and producers;
- **Facilitation of procurement procedures.** Procurers – and where relevant regulatory authorities – would be able to include EU standards and an EU certification as a requirement in their contracts. Furthermore, an EU wide scheme with mutual recognition of certification should support greater openness in procurement procedures by making it easier for potential suppliers

to demonstrate conformity to EU standards/specifications rather than needing to undergo separate national procedures;

- **Reduced uncertainty of compliance with (user) security regulations.** Where procurers/users of security products are subject to regulatory requirements concerning their security arrangements but where these do not specify requirements for specific products/equipment, the utilisation of certified products may support their compliance with legislation.

Impacts on conformity assessment and certification bodies and systems

The potential impacts identified for conformity assessment and certification bodies are:

- **Change in the volume of demand for CAC services.** A single 'one-stop' EU-wide approach should decrease total number of CAC procedures required for each individual product. However, bringing products currently not covered by national CAC requirements within the scope of an EU-wide scheme should increase in the volume of demand for CAC procedures. The overall balance will depend on the actual scope of an EU-wide conformity assessment and certification scheme(s);
- **Increased competition for the provision of CAC services.** For Type-1 products, the introduction of an EU-wide CAC scheme should remove the controlling position that CAC bodies are able to occupy over their national markets, thus promoting competition between CAC bodies. For Type-2 products, the scale of the existing infrastructure for conformity assessment and testing relatively limited, making it difficult to assess the impact of a 'one stop' EU system on competition and on the cost and quality of CAC service provision;
- **Strengthened EU-wide accreditation.** For Type-1 products, it is foreseen that there will be EU accreditation of conformity assessment and certification bodies following common rules and requirements for obtaining accreditation. For Type-2 products, it will be essential that appropriate checks are made to assure the quality and independence of CAC service providers. This implies a strong emphasis on the accreditation of conformity assessment and certification bodies. Accordingly, part of the implementation of an EU CAC system for Type 2 products would relate to the development and operation of the infrastructure and procedures for accreditation of conformity assessment (e.g. testing laboratories) and certification bodies;
- **Increase of administrative costs related to the CAC system.** For Type-1 products it is foreseen that conformity assessment and certification bodies will be EU accredited, which will result in corresponding (additional) administrative costs. For Type-2 products, the introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications would require the development of a corresponding organisational structure. Again, this implies some additional administrative costs.

Impacts on regulators

The main impacts identified for regulators are:

- **Conformity with EU standards as a basis for national regulations.** The development and introduction of European Standards and an EU-wide CAC scheme may make it easier for national authorities to introduce national regulations setting product requirements aligned to these standards;
- **Facilitation of regulations through existence of conformity assessment infrastructure.** The existence of an EU-wide CAC system could remove the need to countries to independently develop such an infrastructure. This may reduce the associated CAC infrastructure costs from introducing regulatory requirements for security products. In turn, this may speed-up the adoption of regulations as there will be lower cost and shorter delay in meeting the corresponding requirements for a CAC infrastructure/scheme to verify compliance with regulations.

Impacts on society

It is conceptually difficult to measure the impact that the introduction of an EU-wide conformity assessment and certification scheme would have on society as a whole and on the security of individuals, businesses etc. This is particularly the case for Type-2 products that address unpredictable security threats. As Type-1 products typically address 'continuous' and relatively predictable security threats, it is to be expected that increasing the performance of security products raises overall security levels and, correspondingly, reduces the negative impact of security 'failures' on society. In this context the following points may be noted:

- **Raised average security performance characteristics of deployed products.** By ensuring that all products meet minimum requirements, an EU-wide CAC system should raise the average performance level of deployed security products. However, there may be risks that an EU-wide CAC system may have a negative impact on overall security performance if it reduces incentives for the development of products with performance characteristics above EU (minimum) requirements;
- **Accelerate the deployment of security products.** To the extent that an EU legislative and CAC 'package' accelerates the deployment of security products (e.g. reduced time to market), particularly to address new threats, it should have a positive impact on security.

Notwithstanding the expectation that an EU-wide CAC system would raise the performance characteristics of security products, the development of an EU-wide CAC system does not remove the fact that security will only be enhanced if the overall systems (including procedures and processes) are appropriate. Thus, the need remains to evaluate broader security systems (e.g. *'concepts of operation'*); including whether the products employed within the system are properly integrated and appropriate given the threat/risk assessment.

1 Extended Summary

1.1 Introduction

This Report describes the findings from the study on “Security Regulation, Conformity Assessment and Certification”, which is the first study undertaken in the context of the Framework Contract on Security (ENTR/09/050) between the European Commission, DG Enterprise and a consortium led by Ecorys Nederland BV. The main elements of the study are as follows:

- **General Framework:** providing a general conceptual framework linking the regulatory environment to conformity assessment and certification of security products;
- **Regulatory Snapshot:** providing an overview of selected elements of the regulatory framework applying to the security sector at national and EU level with a focus on regulations applying to security products;
- **Analysis of Conformity Assessment and Certification procedures:** identifying and analysing the rules and regulations applying to conformity assessment and certification procedures for security products at national and EU level;
- **Options for enhancing Conformity Assessment and Certification procedures:** identifying and assessing possible EU-level options for enhancing conformity assessment and certification procedures.

The analysis of the overall EU situation (as documented in this Main Report) has been supported through national surveys conducted for 7 Member States (Germany, France, United Kingdom, Italy, Netherlands, Poland, Sweden).

1.2 Background and general context

The focus of the study is on two main areas of the general environment (framework conditions) of the security sector, namely the regulatory environment and the environment for conformity assessment and certification in the EU. These two areas have been previously highlighted as of importance for future European security and where EU-level action may be warranted. This is the case, for example, in the Commission’s Communication on "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations" (COM(2009) 691 final):

- With regard to the regulatory framework applying in the security sector, the Communication indicates that: "*ESRIF has underlined that given the fragmentation of the security market, often due to diverging national legislation, a harmonised regulatory framework in specific areas combined with upstream coordination would be advisable. The Commission considers that as a first step, a thorough analysis of the existing regulatory framework is needed*";
- As regards conformity assessment and certification procedures, the same Communication underlined that: "*Based on the requirements of the end-users and the results of research, new technologies and solutions need not only to be validated; they should also be certified and where appropriate standardised, so they can become part of an effective response to security threats. [ ] Meanwhile, the Commission is exploring ways in which the results of relevant research actions could be tested in view of developing future certification / conformity assessment procedures mechanisms. Such mechanisms should aim at certifying that security products and processes are in conformity with relevant standards".*

The above statements from the Commission illustrate the general context and underlying rationale for the study on “Security Regulation, Conformity Assessment and Certification”. Both a more harmonised regulatory framework and improved infrastructure for validating and certifying security products and technologies would provide mechanisms that would contribute to enhancing security within the EU and, by a similar measure, are seen to have the potential to contribute to enhancing the competitiveness of the EU security industry particularly by reducing the current fragmentation of EU markets.

In fact, taking a broad perspective, the highly fragmented nature of the European market has been identified as one of the most significant factors hampering the development of the security industry within the EU. This market fragmentation, contributes to higher costs for European industry and, in turn, procurers and users of security products. It is also part and parcel of a business environment in the EU that some stakeholders argue is potentially unattractive for the future development and long term competitiveness of the security industry. With regard to the relative attractiveness of the EU, attention is often given to the USA, which remains the largest market for security products and which is seen as more supportive of the development and adoption of new and innovative security technologies that serves to reinforce the competitiveness of its security industry. At the same time, weak growth in EU markets compared to growing opportunities in many emerging markets – that often have ambitions to carve out their own positions in the security sector – may further reduce the attractiveness of Europe as a location for future investments in the security industry. From the standpoint of industrial policy, such a situation raises important considerations for future growth and employment prospects in a sector associated with a high potential for technology development and innovation. From a more security and societal standpoint, a possible weakening of Europe’s position in terms of access to, and control over security technological developments in the security field can have important implications for Europe’s future capabilities and independence to provide security solutions that correspond to the needs of its public authorities, businesses and citizens.

1.3 Overview of the regulatory environment for security products

With regard to the regulatory framework, in summarising the present situation, we concentrate mainly on the linkages between regulatory frameworks and other rules relevant to security products and their implications for conformity assessment and certification requirements and procedures. It is evident, however, that this represents only a small part of the overall regulatory environment of relevance to the security sector and that there remain many areas where in-depth analysis may be warranted.

1.3.1 Regulatory background

Over the past decade governments in the EU and worldwide have redefined their civil-security concepts and to develop comprehensive approaches that combine a broad variety of policies instruments and actions. This development reflects the recognition of the security threats posed by regional crises, natural disasters and threats from non-governmental actors, in particular terrorism and organised crime.

At an EU-level, the Internal Security Strategy and, more importantly, the Stockholm Programme of December 2009 provide a broad framework. The EU security model has become a very wide and comprehensive concept taking into consideration risks and threats of any kind that can impact on citizens in a wider perspective and create security problems in a broader sense. For example, the Stockholm Programme focuses on measures that include, for example, improvements in data protection, strengthening cooperation in civil protection, as well as in disaster management and

border control. The recent tsunami in Japan and the ensuing crisis at the nuclear plant in Fukushima are a likely to refocus attention on this wider concept of civil-security.

In attempting to provide an overall assessment of the regulatory framework applying to the security sector at national and EU level and, specifically, regulations applying to security products a number of important features need to be borne in mind:

- At EU-level there is no common (single) framework that applies to security products and the market for security products as a whole. Rather, there are a multitude of different rules and regulations that have been adopted to cover security concerns related to different sectors and activities, and with different purposes:
  - They may directly reflect overarching security requirements; for example, common minimum security levels for airports and ports, or biometric passport requirements to improve identification of persons;
  - They may concern the interface between security and individual rights and privacy; for example data protection rules regarding the processing and movement of personal data;
  - They may be motivated by (internal) market and competition considerations; for example public procurement regulations;
  - The may relate to 'generic' product requirements (e.g. health and safety).
- EU-level and, in many cases national, legislation in the area of security is relatively recent. It is mainly threat driven and follows specific events rather than a long term risk/threat assessment and planning;
- EU-level legislation is limited in scale and scope, with relatively few binding legislative acts that have direct implications for security sector and the supply of (and market for) security products. In general, EU legal instruments contain rather generic provisions that set minimum common requirements for security procedures and only occasionally apply directly to security products;
- Member States retain a degree of flexibility in transposing EU Directives into national law, leaving room for interpretation. Further, national governments typically retain the prerogative to impose more stringent security requirements. Thus, national differences in rules and regulations, which may be well justified on individual country's security threat assessment, can and do contribute to market fragmentation.

1.3.2 Regulatory situation by area

After the above introductory remarks on the general regulatory framework, the following subsections outline the regulatory environment – with specific reference to the linkages between regulatory frameworks and other rules relevant to security products and their implications for conformity assessment and certification requirements and procedures – in some key areas that illustrate the current fragmentation of EU markets.

Aviation (airport) and Maritime (port) security

The international and EU-level regulatory frameworks are quite comprehensive with respect to aviation (airport) and maritime (port) security. In this regard, however, the EU regulatory frameworks have the ambition of ensuring common minimum levels of security, leaving open the possibility for divergent national situations where the security situation of individual Member States warrants more stringent requirements than implied by the EU minimum requirements.

EU regulations for aviation security provide a framework for the definition of detailed technical specifications required for some categories of security equipment (cf. screening equipment for passengers and luggage) and consequently, imply the need for corresponding conformity assessment (validation) processes. The regulatory framework does not, however, provide for a common EU conformity assessment and certification/approval scheme. Different national

regulations persist, and it remains the case that national authorities may complete EU-defined security equipment 'standards' with specific national requirements.

Despite efforts towards a common evaluation processes for security equipment, such as the ECAC CEP[1], final approval of airport security equipment remains a national decision. The lack of harmonised security technology standards and common criteria for the validation of air transport security equipment – and, more broadly security solutions and services – leaves the market open to fragmentation. However, the struggle to arrive at an agreed approach to the utilisation of security scanners in airports is illustrative for the problems associated with achieving a common EU-wide position and common standards for security equipment. Moreover, it can be noted that the EU regulatory framework which defines a list of eligible methods and technologies for passenger screening can provide a barrier to the introduction of new technologies. Airports are not permitted to replace systematically any of the recognized screening methods with alternative technologies until they are added to the legally binding list of eligible methods; this has presented a barrier to the introduction of LAG (liquid, aerosol and gel) screening and security scanners ('body scanners').

Regarding port security, regulation sets requirements for the designation of port security authorities, which are responsible for identifying and taking the necessary port security measures. Commission security inspections of port facilities and companies are carried out with assistance from the European Maritime Safety Agency and are conducted by inspectors from the Member States. Although there are currently a large number of new technologies being developed (e.g. for maritime surveillance), they are at an early stage and current legislation does not require their use: consequently, there is no common framework for conformity assessment and certification.

Other Critical Infrastructure Protection (electricity and urban transport)

In areas of critical infrastructure protection – for which the national surveys focus on electricity generation, transmission and distribution and urban transport – there is a much weaker EU-level regulatory framework. Partly this reflects the limitation that EU-level initiatives have been largely limited to 'European' critical infrastructures having a trans-national dimension. Moreover, EU guidelines concerning common terms, approaches, methods and requirements etc. are lacking. Overall, this means that regulatory frameworks are mainly defined at national and sub-national levels (e.g. for federal/regional structures), with implementation obligations often devolved to local-level administrations.

A particular area of concern is the vulnerability of ICT systems – which in themselves can be considered critical infrastructure – associated to critical infrastructures. There is a perception of a real and growing threat of cyber-attacks targeting critical infrastructure IT networks. At the same time the EU market for ICT / cyber-security is wide and unstructured, and in relation to Critical Infrastructure viewed as insufficient and often fragmented at a national level. While the Commission Communication on Critical Infrastructure Protection (COM(2009)149) represents a step forward, there is still no EU-wide legislation in this area.

In the field of urban transport, there appears to be an equally unstructured and fragmented market with many decisions relating to security being taken at a local level. One area of interest from a security equipment point of view concerns CCTV surveillance in urban transport environment and is illustrative of local-level fragmentation of security markets. On the one hand, there has been progress made over the last years in the development of European Standards (EN) that cover CCTV used for security purposes. However, there seems to be little evidence of the consistent

[1] European Civil Aviation Conference (ECAC) Common Evaluation Process for security equipment (CEP).

application of these standards at national (or local) level, or in requirements for CCTV systems used in urban transport environments to conform to these EU standards. On the other hand, the utilisation of CCTV, in particular from the perspective of data protection and privacy, is subject to a wide array of different national regulatory systems. The diversity of legislation combined with the fact that legal frameworks are seen to lag behind rapid technological developments, suggests that efforts towards EU harmonisation may be warranted.

Border security

The general framework for border security is influenced by pattern of participation of Member States in border security arrangements, notably the Schengen agreement and *acquis*. This can be remarked in relation to participation in the three large scale information technology systems in this area. Ireland and the UK participate in EURODAC (European database of fingerprints) but are only partly involved in SIS II (Schengen Information System), and do not participate in VIS (Visa Information System); Denmark is involved in all three systems but on a specific legal basis. While the legal framework is characterised by a 'variable geometry', it is unclear whether this contributes to fragmentation of the EU market for security products.

Following the 9/11 attack in 2001, Member States were asked by the Commission to take immediate action to improve document security, resulting in the integration of biometric identifiers in passports and other travel documents. In accordance with international standards, the Commission established additional technical specifications (e.g. additional security features, storage medium and its security, common quality criteria for facial images and fingerprints). A comparison between the regulatory framework and supporting initiatives taken to support the development of EU-wide approaches for conformity assessment and certification for biometric passports (and identity cards) and the approach adopted for automated border control systems provides some interesting insights into the contribution they can make towards overcoming potential market fragmentation:

- **Biometric identity cards:** Based on an international agreement, EU Regulation 2252/2004 requires the introduction of biometric identity cards, which can be read electronically across all EU countries. Using an international technical standard developed by ICAO the EU developed an EU norm specifying the type of biometry, chip and the functionality required. Tests and certification are carried out on the basis of ISO scheme 15408 with common criteria for the tests. In addition, the Commission together with the Joint Research Centre (JRC) has facilitated several interoperability tests where all identity card manufacturers were tested against suppliers of reading equipment. This model is seen as 'best practice' by stakeholders comprising, as it does: a worldwide (basic) standard; EU regulation; EU certification scheme; and EU facilitation to bring together suppliers along the security value chain;
- **Automated border control:** The original initiative(s) providing for automated border control came essentially from the private sector. After the authorities had agreed to open up the security function of automated border control (passport control), (quasi) private companies drove the process in very different directions without much consideration for issues of standardisation and conformity assessment. Currently, each of the four automated border control projects in the EU[2] has its own requirements, standards and time line. Importantly, interoperability is not asked for, since automated border control is considered as a strategy to achieve a completive advantage for airports. This model is seen to contribute to fragmentation: no EU Regulation; no EU technical specifications but rather proprietary solutions; no published information on the requirements set by the operators; no prescriptions for the need of conformity assessment; and no facilitating role of the EU.

[2] The 'Iris' programme in Heathrow, UK; The 'Mysense' project in Schipol, the Netherlands; The HBG at Fraport, Germany; and The 'Pegase' programme in CDG, France.

Export controls and public procurement

The EU Directive of the procurement of defence and sensitive security supplies, works and services (2009/81/EC) aims to bring public procurement more closely into the Internal Market and to open up national markets to competition. The provisions of the Directive are such that it can be supplied across the entire spectrum of security related public procurement, and it is clearly the intention that this may involve, for example, border protection, police activities and crisis management missions. Currently, Member States are still in the process of transposing the Directive into national legislation and so it remains to be seen to what degree it will open up national security markets to competition. In particular, it is unclear to what extent Member States may apply the various exclusions, which are particular relevance for 'sensitive' security products. Further, it remains to be seen whether companies bidding for security (and defence) equipment and service contracts will be prepared to challenge Member States (routine) use of Article 346 TFEU (Article 296 TEC) exemptions.

Data protection and privacy

The regulatory environment for data protection in the EU including, as it does, reference *inter alia* to the Charter of Fundamental Rights and the European Convention on Human Rights, is worthy of a separate study. The Data Protection Directive (95/46/EC) provides for protection of individual rights with respect to the processing and free movement of personal data; though defence, public security, state security and the activities of the state in criminal law are outside the scope of the Directive. However, with the abolition of the 'pillar structure' through the adoption of the Lisbon Treaty, the Commission intends to include provisions in a revised Data Protection Directive that will cover police and judicial cooperation in criminal matters. The current Directive leaves Member States the possibility to go beyond the minimum requirements set by the Directive. While each Member State has codified the Directive into law, the interpretation, exemptions and enforcement vary from state to state. This means that despite the Directive, there is a lack of harmonisation across Member States. Furthermore, verification of conformity of IT (and other) equipment and systems with data protection and privacy requirements remains an important issue. Currently, more needs to be done in order to provide independent verification/certification of the compliance of technologies, products or services with legal requirements for data protection.

1.4 Overview of the conformity assessment and certification (CAC) environment for security products

1.4.1 Conformity assessment and certification background

With regard to existing CAC frameworks, two main areas of concern have been identified:

- **Absence of common certification systems** for security products at a European level and no mechanism of mutual recognition across countries of products certified at a national level;
- **Slow speed of response and adaptation of certification procedures** notably where new security threats require the implementation of new security solutions and technologies. As a consequence technologies may already be out-dated before approval and certification procedures are implemented.

These concerns are illustrated in the following subsections that outline existing approaches to CAC related to security products. In general, such concerns point to the potential for EU-wide policy initiatives to improve conformity assessment, testing and certification of security products, by enhancing approvals and certification procedures and infrastructure. A general objective of such initiatives could either be to generate new certification strategies or harmonise existing ones, with the aim of ensuring that CAC frameworks are adequate to meet EU requirements. Moreover, moving to greater mutual recognition between countries, increasing transparency of procedures,

and improving the level and quality of interaction between approval and certification bodies could raise the efficiency of the system and support EU security technology development.

1.4.2 *Current approaches to conformity assessment and certification*

EU 'generic' approach under the New Legislative Framework

The general EU framework for conformity assessment and certification of products is contained within the New Legislative Framework (NLF). To date, the use of the NLF has mainly related to aspects such as protection of health and safety of products but also including electromagnetic compatibility. Some categories of security-relevant products are, however, covered by the Construction Products Directive/Regulation which follows a NLF approach; however this relates to products that are typically somewhat removed from the types of threats normally associated to major civil-security concerns. Otherwise, security-related requirements for products have not been handled through a NLF approach and the utilisation of the NLF to cover requirements related to security aspects and performance of products (and services) is an issue open to further scrutiny. Nonetheless, in principle at least, the NLF could form the basis for any future regulatory approach used to set *inter alia* performance requirements for some security products and technologies.

Supra-national approaches in the security domain

Moving away from 'generic' approaches to conformity assessment and certification, it is important at the outset to note that in most instances current approaches – particularly where they concern supra-national schemes – are in many cases relatively new. Accordingly, their lack of maturity makes it difficult to assess their relative strengths or weaknesses. The current situation may be summarised as follows:

- **General / 'Traditional' security equipment.** A limited number of security-related equipment (e.g. fire alarm and fire protection equipment) are covered within the scope of the Construction Product Directive/Regulation and, thus, fall with the provisions for mutual recognition of certificates of compliance with EU regulations. Otherwise, for what may be termed 'traditional' security equipment (e.g. intruder alarms, access control, CCTV surveillance, etc.), the EU market is characterised by national schemes for conformity assessment and certification. Where certification is required – and such requirements are by no means common across Member States – suppliers must usually submit to local conformity assessment and certification procedures. There has been very little progress towards common certification schemes and/or mutual recognition of certificates and efforts such as the CertAlarm scheme, which has the ambition to provide an alternative EU-wide certificate for 'traditional' security equipment, has only recently started and it is too early to assess how the scheme may develop in the future;
- **Priority / 'New' security equipment.** Regulation of the aviation sector and biometric identification are among the clearest examples where legislation sets (performance) requirements for security products. In both these areas, however, it can be remarked that there is not a complete harmonisation of performance requirements across countries and, consequently, differences in national conformity assessment and approval/certification. Also noticeable is the limited scale of the infrastructure for undertaking testing of these categories of security technologies: there are only four test centres in the EU that test and certify biometric equipment; similarly, in the aviation sector, under ECAC CEP there are only 4 test centres for Explosive Detection Systems (EDS) and 3 centres for Liquid Explosive Detection Systems (LEDS). With regard to other sectors covered by the study – maritime/ports, urban transport, and other critical infrastructure (e.g. power generation, transmission and diffusion) – most supra-national regulations are pitched in terms of requirements for overall security procedures and processes; for example through requiring the designating of security authorities and requiring the Member States to ensure the appropriate security plans are developed. Typically,

such regulations do not set out performance or other technical requirements for security products;

- **IT security and data protection.** The development of common and supra-national approaches to conformity assessment and certification is often a reflection of the presence of a multitude of differing national approaches. For example, the Common Criteria for Information Technology Security Evaluation - Common Criteria (CC) for short - are the outcome of the efforts of a number of governments (USA, Canada, UK, France, Germany and the Netherlands) to develop harmonised security criteria for IT products. However, the CC are seen by some to be too slow and too bureaucratic to respond to rapidly changing developments in information security technologies; in part because they rely on consensus for the development of new standards. It appears that there is some slippage in the use of CC evaluation procedures with certain countries pushing their own national testing regimes.

Insurance-related frameworks for conformity assessment and certification

Moving away from the regulatory environment, the insurance industry historically had an important influence on the development of conformity assessment and certification requirements for security products. This is most evident in relation to 'traditional' security products for which the insurance industry has fostered the development of standards for safety and security products. In turn, this has been accompanied by the development of corresponding (national-level) conformity assessment and certification procedures. While the scope of security equipment and technologies covered by this kind of certification does not accord with some of the 'high-level' security threats and environments that are identified as priorities from an EU-level perspective, the role of the insurance sector nonetheless warrants attention for several reasons:

- There are sources of standards and for conformity assessment and certification of security products outside regulations;
- The development of some standards and certification schemes might require, or might purposefully use, the dynamics created by the interaction of private market participants (insurance and re-insurance companies and "their" certifying bodies) to provide for a quick and adequate reaction to technological innovations;
- Insurance companies and "their" certifying bodies represent important stakeholders for CAC in the security sector. At national level, the latter have devised – independently or in collaboration with national standards authorities – numerous standards and hold a firm hand on their domestic certification market.

One issue with regard to the role of the insurance sector in relation to CAC or security products is that existing frameworks are essentially nationally organised, with little mutual recognition of certificates between countries. Certifying bodies linked to the insurance sector have been slow to embrace EU-wide solutions, a development that has only started recently. One reason is that national regulations typically make reference to national rather than to EU standards and in some cases EU standards do not exist or are less stringent than national standards. Furthermore, to some extent it appears that in the past the security industry has at least tacitly accepted the dominance of national certification bodies, as it provided a degree of support for domestic security products in home markets and also in export markets where the label of the certification body was widely recognised as a mark of quality. Overcoming the entrenched position of national certification bodies would, therefore, be an obstacle to be overcome in any initiative towards an EU-wide system for CAC.

While the above discussion relates to the use of approved/certified security products, a further dimension to the interrelationship between CAC and insurance is concerned with the supply of products and the liability of the providers of security equipment in the event of a security incident. A particular issue is the third-party liability of security equipment (and service) providers. There

appears to be a high degree of concern on the side of industry that present rules within the EU leave it exposed to potentially unlimited third-party liability in the event of a major security incident. Moreover, it is claimed that the insurance market does not currently provide industries with comprehensive options or solutions to meet such exposure.

1.5 Key issues relating to the rules, regulations and procedures for conformity assessment and certification of security products

The analysis undertaken by the study, including engagement with stakeholders, has identified a range of issues concerning the regulatory and general environment for conformity assessment and certification in the security sector, which seem relevant for the identification and assessment of possible approaches and EU-level options to enhance current CAC procedures. Some of the key issues are outlined in the following sub-sections.

1.5.1 Governance aspects

National specificities versus common approaches

While there may be broad agreement at an EU-level on the general nature, scope and perceived magnitude of the main civil-security threats, when considered from a specific local or sector context these can translate into more heterogeneous security situations and corresponding requirements. Differences in national (and local) situations, security challenges, and preoccupations, provide grounds for arguing that ultimately the evaluation of security threats can only be undertaken at a national level; a position that is reflected in EU legislation (e.g. provisions for Member States to impose stricter security requirements where deemed necessary). This, however, reduces the possibilities to develop and 'impose' EU-wide standards and CAC requirements in so far as they relate to the 'security' and certain 'operational' characteristics of products, as opposed to other aspects such as interoperability requirements.

Administrative and regulatory responsibilities

The rules and regulations setting the conditions of supply and utilisation of products in relation to civil security are determined at different administrative levels from supra-national, via national and regional, down to very local levels (e.g. municipal authorities). While it is the case that international (including EU) frameworks for civil security exist in certain sectors (e.g. aviation and maritime), it is often the case that many responsibilities for civil security remain at a national-level and are even further devolved to regional and local levels. There is an obvious logic behind the argument that local actors may be better placed to evaluate security conditions and requirements. However, this implies that the prescription of security needs and the corresponding conditions applying to the application and utilisation of security products are in many instances set by local actors. Accordingly, fragmentation of markets within the EU is not simply a question of differences in national regulations, rules and requirements but also of fragmentation within national markets.

Market organisation and institutional arrangements

The security market embraces a range from primarily institutional market segments – reflecting public sector responsibilities for civil security – through to essentially private sector market segments. In the middle of this range is something of a grey area where boundaries between public and private sector responsibilities can be blurred. This is particularly evident in respect of several key infrastructure segments that have been characterised by a transfer from public to private sector ownership and operator responsibilities. In general, the transfer from public to private ownership implies that, whereas in the past a single entity (i.e. the government or a government agency) was responsible both for the determination of security requirements and their implementation, these

functions are now separated. In an environment in which operators are subject to competition and shareholders' scrutiny of their performance, this separation can create conflicts in terms of who should meet the financial implications of security. Moreover, the break-up of traditionally integrated infrastructure and service providers into multiple operators can in itself result in fragmentation of the market, particularly where there is a lack of coordination of security approaches and functions between different entities.

Public versus private-sector led initiatives

There is a tendency to focus on the role of public authorities and regulatory requirements as the key driver of security markets; this reflects the ultimate responsibility of public authorities for ensuring civil-security, particularly with regard to key challenges such as terrorism, organised crime and disaster management. In general, however, public authorities have tended to focus on overall requirements for security which, in turn, has increased attention of standardisation issues, notably in relation to emerging security technology. By contrast, with exception of initiatives in the area of IT security and for specific product categories (e.g. airport scanners, e-passports), conformity assessment and certification issues in these areas have generally received little attention from public authorities.

From a historical perspective, much of the drive for development of standards and conformity assessment and certification procedures for 'traditional' security products has come from the insurance sector. While the preoccupations here are less associated to EU 'priority' security challenges (e.g. terrorism), they are nonetheless relevant in terms of influencing standards and third-party certification requirements for many categories of security equipment (e.g. intruder alarms, access control systems, surveillance systems).

In addition to the above, the supply-side can also drive the development of standards and associated conformity procedures, particularly in relation to interoperability requirements for new and emerging technologies. What distinguishes such initiatives is that there tends to be less attention to independent (third-party) conformity assessment and certification and more attention to self-declaration of conformity to industry standards and compliance to codes of practice.

Limited involvement of end users and other stakeholders in the elaboration of standards

While there is an underlying principle that standards should be developed on a 'consensus' basis, in many areas there appears to be little involvement of end-users. Standardisation bodies, certification bodies, technical experts (that may themselves be part of the CAC infrastructure) and other stakeholders such as the insurance industry tend to comprise the main participants in the development of standards, with lower representation of end-users.

EU level lead for newly developed equipment

There have been a number of cases where security functions were opened up to automation or new technology had to be developed to address new threats. In these cases EU level leadership can contribute to ensuring that a single market across the EU rather than a number of national markets emerge. While private actors such as airports, airlines (or in the future ferry companies and ports) might want to seek a competitive advantage and therefore lead the introduction of such new technologies, early EU action may be required as to ensure a common level of security across the EU and to avoid market fragmentation.

1.5.2 *Approaches to, and scope of, regulation and CAC processes for security products*

Product-based regulation versus obligations and conditions of use for security products

The regulatory framework relevant for security products can be based on differing approaches:

- **Product (supply) based.** Legislation may apply directly to a certain category of security product, setting out 'blanket' conditions (e.g. minimum technical specifications) to which the products must conform in order to be made available on the market; this is the case, for example, for generic 'health and safety' requirements. Typically, some form of product testing is required to verify compliance with such '*product-based*' legislation[3];
- **Sector (demand) based.** Legislation may apply to the customers and end-users of security products; for example where security requirements are set for specific economic sectors or activities[4]. Such regulations are limited to setting obligations on the relevant 'actors' – either public or private sector, or both – to ensure adequate measures are implemented to maintain security; for example, as is the case for port security. Typically compliance with such '*sector-based*' legislation is based on inspection and auditing of security procedures of conformity-assessment;
- **Hybrid 'sector-product' based.** A 'hybrid' of these approaches is provided where legislation not only sets out obligations to fulfil certain security functions but, also, sets out the relevant means (and technical specifications thereof) through which the security function is to performed. This is the case, for example, in the case of passenger and luggage screening in the aviation sector.

To date, the main thrust of security-related regulations has been of the second type listed above. Security regulations are typically orientated towards a particular type of (economic) environment (e.g. aviation, maritime, critical infrastructure, etc.) or activity (e.g. border control, management and transport of hazardous materials, etc.). As such, regulations do not directly provide technical specifications for security products, leaving the evaluation of the appropriateness of employed products/technologies to the discretion of the relevant authority or inspectorate. Further, this leaves open the possibility that other instruments – e.g. administrative circulars and guidelines, advice notes, codes of practice, voluntary agreements – that recommend the use of given specifications or standards, can set compliance requirements that though not mandatory can become *de facto* obligatory.

Standards and CAC for single equipment versus systems

Existing performance standards and corresponding CAC arrangements are at the level of individual equipment and components. Many stakeholders point to the need for systems approaches that look at systems that combine different equipment (e.g. complex checkpoint solutions) and that also take into account the provision of services that are directly linked to products/equipment. Conformity of individual products/equipment does not ensure the effective provision of security. Individual products/equipment need to be able to 'communicate' and 'collaborate' with other products/equipment in the system; and the system often has to be connected to service personnel (e.g. security service providers, police) to provide effective security protection and response.

Certification of products versus certification of systems

Following from the above point, addressing conformity assessment and certification requirements for complex systems raises issues related to which of the parties are positioned to obtain approval/certification. For individual products it is evidently possible for the manufacturer/supplier to

---

[3] Such legislation can specify the applicable mechanisms for determining conformity with the requirements, including by whom the activity is performed (e.g. manufacturer, user, independent conformity assessment body) and the form in which the declaration of conformity is made (e.g. self-declaration, third-party certification).

[4] This may also include legislation and regulations relating to public procurement.

obtain approval/certification of their product. However, when dealing with large systems that integrate equipment from different suppliers and/or where the configuration and operational characteristics are specific to the particular environment in which the system is deployed, either the system integrator (where there is one) or the actual operator will need to obtain approval/ certification of the system. In this regard, given that large systems are more closely linked to the environment in which they are deployed, it is probably more difficult to harmonise certification of systems, than it is to harmonise certification at the individual product level.

Privacy and data protection issues

The on-going debate over the use of security scanners highlights the role of 'ethical' issues such as privacy and data protection. In the absence of a clear European framework in this area and at national levels also, there is an absence of clear guidelines for equipment/technology providers with respect to accepted and acceptable performance requirements. A similar situation exists with respect to protection of personal data collected and held by biometric identification systems, for which national approaches and requirements vary significantly.

Certification not appropriate for all conformity assessment issues in the security sector

Conformity assessment in the security sector is sometimes done on the basis of a classified 'standard', as for example in the case of security plans for ports or airports or the performance criteria in case of some ECAC tests. Here the classified character of the 'standard' contributes to the security function. In these cases the integrity of the conformity assessment processes is of critical importance and may limit the scope for assessments to be conducted by private certifying bodies for two reasons: on the one hand, this would increase the number of people who would require access to the information; on the other, certifying bodies are often private companies operating in a market and their incentive structures might lead to a conflict of interests to the task they have to carry out. Both aspects do not only increase the risk but also call for additional checks on the reliability of the certifying bodies.

Confidence in CAC frameworks

Any efforts towards common EU approaches for CAC must be able to guarantee confidence in the 'quality' and 'independence' of approvals and certification outcomes. In particular, this relies on the strength of mechanisms for accreditation of conformity assessment bodies and, in particular, test laboratories (and other similar organisations) responsible for verifying conformity. In this regard, the limited number of suitably qualified testing laboratories suggests that there may be capacity constraints with existing CAC infrastructure.

1.6 Framework for establishing potential EU-level approaches for conformity assessment and certification of security products

1.6.1 Categorisation of security products

In defining possible options for CAC for security products, account needs to be taken of the wide diversity in security threats and corresponding capability and performance requirements; in security products and security technologies; and in security markets, both in terms of economic sectors/activities and categories of customers (institutional, private, etc.), and in the 'drivers' shaping demand. While interaction of such factors implies a complex set of market conditions, the general situation can be characterised in terms of two contrasting market-product segments that illustrate the differing challenges for any EU initiatives towards conformity assessment and certification:

- **General purpose security products (Type-1):** security products and solutions aimed at addressing 'familiar' security situations (security threats or functions) through the application of

improved but existing technology. This includes what may loosely be called 'traditional' security equipment (e.g. intruder detection, CCTV, access control, security barriers);

- **Priority and sensitive security products (Type-2):** security products and solutions addressing 'unfamiliar' or new types of threats that often require the development or application of new technologies and approaches. This latter category may be extended to changes in organisation and implementation of security functions; for example through the automatisation of security functions. This includes what may loosely be called 'new' security equipment (i.e. corresponding to products/technologies developed primarily to address threats such as terrorism, organised crime, cyber-crime, etc.).

1.6.2 Main policy challenges by security market-product segment

Using the two market-product segments outlined above the main policy challenges relating to the rules, regulations and processes for conformity assessment and certification may be summarised as follows:

- **For Type-1 products,** the main policy challenges stem from the absence of common EU-wide certification of products. Manufacturers and suppliers point the fact that they are faced with *de facto* requirements to separately certify products in almost all EU countries as there is no – or very limited – recognition of certification between countries. In this regard, they argue that certification bodies have been slow to embrace EU-wide solutions that would reduce or remove the need for multiple national certifications. As a consequence, manufacturers and suppliers face the administrative burden and cost associated with multiple certifications of their products which, particularly for SMEs, represents a significant barrier to supplying new markets. Certifying bodies counter that the market demands for national certification are associated more to the lack of acceptance and use of European Standards; either because harmonised European Standards do not exist, are not familiar to market actors, or do not meet specific national exigencies;
- **For Type-2 products**, the range of policy challenges is wider, since there is often a direct link to issues of EU Internal Security, including ensuring minimum security performance levels (and promoting higher ones) and speeding-up the deployment of new technologies and solutions. Here, in combination with the development of common EU standards for performance (and other aspects such as interoperability), a common approach to conformity assessment and certification could contribute to reducing/avoiding the fragmentation of newly emerging market segments in the EU. An EU wide CAC system – based on common performance criteria – should increase market transparency by providing end-users with greater information on the relative attributes of different products and, hence, promote competition.

1.6.3 Characterisation of potential EU-level policy approaches for CAC of security products

Using again the two market-product segments outlined above, the main elements and issues to be addressed by possible policy actions to enhance existing frameworks for conformity assessment and certification can be summarised as follows:

- **For Type-1 products**, for which there exist performance and other technical standards – albeit differing at national levels – and national infrastructures for testing equipment in many Member States:
  - **Standards harmonisation:** The first focus for EU policy intervention would relate to the development of harmonised European Standards and the promotion of their use within the market (see next bullet point). The adoption of harmonised European Standards would provide the basis for EU-wide certification, either through mutual recognition of national certification or certification through an approved EU-wide sector scheme;

- **Market recognition of European standards:** The second focus for EU policy intervention relates to the extent of market recognition of products certified as conforming to European Standards. On the one hand, the market may recognise European Standards and duly certified products without the need for further EU intervention; i.e. a voluntary solution is achieved. On the other hand, if there is continued insistence on national certification then additional EU intervention may be justified. This could include non-legislative initiatives to promote recognition of European Standards and EU-wide certification with relevant markets actors;
- **Regulation:** A legislative approach may be adopted if a market-based solution resulting in common (EU-wide) certification or mutual recognition does not develop. This could take the form of the introduction of specific legislation for security products following, for example, a NLF approach that would prevent Member States from prohibiting the placing on the market of security products that have been certified by a competent (notified) conformity assessment body in another Member State;
- **Conformity assessment and certification:** Notwithstanding whether a market-based or legislative approach is adopted, existing accreditation procedures and conformity assessment infrastructures (e.g. testing laboratories) could be used to provide conformity assessment (testing) services and certification in accordance with the – to be developed – harmonised European standards.

- **For Type-2 products**, consideration needs to be given both to the process of defining EU standards, including those related to testing methodologies and test criteria, and to the overall design of an EU system for conformity assessment and certification. In this regard a number of issues arise:
  - **Regulation:** As described earlier, relevant EU regulatory frameworks can be characterised as product (supply) based or sector (demand) based, or a hybrid combination. A sector-based approach for CAC would complement existing sector-based regulatory frameworks but would be limited only to the sectors covered by legislation. A product-based approach to CAC would provide a general system of approval/certification of categories of products but would need to address possible variations in requirements for different sectors/activities. From a legislative perspective it would arguably be easier to follow a sector-based approach, since this would enable Implementing Acts – setting out technical requirements and CAC procedures – to be 'attached' to existing sector-based security-related regulations. However, if the overriding concern is to reduce market fragmentation within the EU and across sectors then a product-based or technological-based framework may be preferable, since this would create a single system of CAC for product categories, irrespective of the sector in which they are deployed. This would require new Legislation setting essential (and technical) requirements for categories of security products and may be less rapidly introduced than Implementing Acts attached to existing regulation. However, ultimately, a product based approach could lead to a more harmonised overall approach for CAC;
  - **Standards:** A basic principle for CAC is that it should demonstrate conformity to recognised standards (preferably international or European) or other transparent and objective criteria – such as technical regulations – in a non-discriminatory manner. Similarly, when setting performance measurement standards, the measurements or test results should be traceable to recognised (preferably international or European) measurement standards. These conditions pose a number of difficulties with respect to Type-2 products, particularly for new technologies for which recognised standards may not exist. This may be a specific problem where deployment of the product is immediately or imminently required (for example, in response to the evolution of security (terrorism) threats). Furthermore, security performance requirements and associated test criteria can be 'sensitive' (e.g. classified or secret) information, making it more difficult to provide transparency and ensure objectivity while,

also, requiring protocols for information confidentiality that may influence the definition of a CAC system;

- **Accreditation:** A common EU CAC system for security products would have to command the confidence and support of Member States throughout the EU, thus enabling the principle of mutual recognition to be accepted (i.e. Member States recognition of certification received from another Member State or, possibly, a central EU Certifying Body). In order for Member States and other stakeholders to have confidence in the CAC system and procedures, adequate and appropriate 'checks and balances' would be required to assure necessary expertise of conformity assessment bodies (e.g. testing laboratories) and to assure that applied conformity procedures are appropriate (e.g. test criteria and methodologies utilised by the laboratories are adequate to demonstrate conformity with the specific technical requirements set for a given product category);
- **Certification:** One of the main aims of a common EU CAC system for security products would be to remove (or at least reduce) the need for multiple national approval/certification of security products. A fundamental question is, therefore, the extent to which national authorities would be prepared to accept the principle of mutual recognition of approval/certification by another Member States. An alternatively may be to adopt a more centralised approach with approval/certification being issued by a single organisation subject to specific scrutiny by the EU with, or on behalf of, national authorities. Nonetheless, for some product categories it has been indicated that, irrespective of the reliability and integrity of an EU-wide CAC system, Member States may consider that they have an essential obligation to undertake their own national testing and validation of certain categories of security products.

In terms of the institutional structure necessary to support CAC of security products, for Type-1 products it would seem appropriate to build on existing CAC schemes. For Type-2 products associated with specific regulatory responsibilities (and expertise) and that require specialist technical expertise, a dedicated CAC scheme and infrastructure is more likely to be necessary.

1.7 Definition of possible EU-level initiatives to enhance conformity assessment and certification of security products

1.7.1 Outline of policy options

For the purpose of identifying and assessing the potential impacts of possible EU-level initiatives to enhance conformity assessment and certification of security products, a limited number of policy options have been defined. These options reflect the requirements set in the terms of reference for this study and the outcome of consultation of stakeholders and interaction with the European Commission. These options are summarised as follows:

- **Option 1 - Baseline.** This scenario represents a continuation of the currently existing situation. Here, no common EU-wide system providing conformity assessment and certification (CAC) of security products would exist. Security products subject to approval/certification requirements would continue to undergo national testing, validation and approval/certification procedures. No priority would be given to certain products. Furthermore, no additional development of EU-level structures and processes for the implementation of conformity assessment and certification requirements and procedures would take place;
- **Option 2 - A step by step approach.** This option would apply to the two market-product segments described above (i.e. Type-1 and Type-2) and would consist of two sub-components:
  - ***Option 2.1** - EU CAC for 'general purpose' security products (Type-1).* Intended to cover security products aimed towards 'general' security markets and/or based on comparatively mature technologies (Type-1);

- ***Option 2.2*** *- EU CAC for 'priority and sensitive' security products (Type-2).* Intended to cover security products aimed either towards 'specific' markets and/or based on comparatively new or innovative technologies (Type-2);
- For each product type it is assumed that a step-by-step approach would be adopted under which EU initiatives would start with limited product category coverage, to be expanded over time and in response to changes in security-based and market-based priorities. Criteria for the prioritisation of product categories are discussed in the following subsection.

- **Option 3 – An all-encompassing approach.** This would be a situation where an EU-wide CAC system is in place for all security products (both Type-1 and Type-2) all at once. No staging of the introduction of CAC for different product categories / technologies is foreseen.

1.7.2 Prioritisation of security products and technologies to be covered by an EU-level CAC schemes

Policy Option 2, outlined above, assumes a step-by-step approach that would incorporate a prioritisation of security products and technologies to be covered by EU-level initiatives for conformity assessment and certification. Accordingly, consideration of the possible relevant criteria that may be utilised for prioritising products and technologies is required. In this context, possible criteria may be identified in relation to the main policy challenges (policy areas), as follows:

- **EU Internal Security Policy:** from a security perspective the overriding concern is to ensure the rapid and effective deployment of security products/technologies to ***address the most pressing security threats and challenges***. This requires linking information on security threat assessments and scenarios to capability requirements and corresponding security product/ technology development and deployment. Evidently, detailed information on current threat assessments is not in the public domain, thus making it difficult within this Report to identify those products and technologies that would be priorities from the perspective of EU Internal Security. However, in a more general context, existing analysis such as the work undertaken by ESRIF provides some indications of priority areas for technology development and innovation in the area of security. The on-going developments in these priority areas (i.e. closeness to actual deployment of 'new' solutions) suggests the need for an on-going 'technology watch' to monitor security technology developments and innovations. A link may also be made to public funding programmes (e.g. EU Framework Programmes and Member State's research and innovation support), perhaps to the extent of including consideration of possible CAC requirements within the scope of projects;
- **EU Internal Market Policy:** from an internal market perspective the main consideration is to reduce the existing fragmentation of markets within the EU. Accordingly, the main criteria for prioritisation of security products and technologies to be covered by an EU-wide CAC scheme would relate to the ***prevalence and magnitude of barriers to trade*** and to the extent to which there is a lack of a 'level playing field' within the EU;
- **EU Industrial Policy:** from an industrial policy perspective, two criteria for prioritising products and technologies to be covered by an EU-wide CAC scheme come to the fore. Firstly, the potential to ***reduce costs and administrative burden*** placed on manufacturers/suppliers of security products as a result of existing CAC requirements (e.g. multiple certifications). Second, the potential contribution that an EU-wide scheme could make to enhance the competitiveness of the EU security industry. Concerning this second criterion, two particular elements may be identified. On the one hand, the benefit to the EU security industry can be expected to be greater for those product categories and technologies where ***EU industry has a comparatively strong market position*** and for which a more unified market within the EU could serve to reinforce this position (e.g. strong 'home' market as a support for international/global competitiveness). On the other hand, the potential benefits that may come from developing EU-wide CAC schemes that also ***support technology development and innovation*** by EU

industry, particularly in those areas where market opportunities (both within the EU and globally), are expected to be strongest.

The above discussion highlights certain criteria that may be used to identify priority security products and technologies starting from a policy-area based approach. To these some more practical and pragmatic considerations that may influence the prioritisation of products/technologies to be covered by an EU-wide CAC scheme, are:

- **Speed and ease of implementation:** an EU-wide CAC scheme may be more quickly implemented and show effective results if it is able to build upon existing CAC infrastructures and where recognised standards already exist or can easily be developed. In the case of Type 1 products, for example, some schemes for pan-European certification already exist (e.g. CertAlarm) that could provide the basis or template for an EU-wide CAC scheme. Also, European Standards (EN) have already been established for some products and components. Accordingly, an EU-wide CAC scheme may be relatively easily introduced and could be expected to have a rapid impact on the sector/market;
- **Long term benefits for industry, customers and citizens:** developing an EU-wide CAC scheme for products and technologies addressing many 'priority' security challenges may require more time to implement and to demonstrate its effectiveness but may yield greater 'benefits' in the longer term. In the case of Type 2 products, for example, it is typically the case that recognised standards do not exist and that existing CAC infrastructures are relatively limited. Moreover, Type 2 products covers more complex equipment and larger security systems the deployment and operation of which is often specific to a particular environment/context. This may require approaches for CAC that are not based on individual products (i.e. no "one fit for all" approach) but may necessitate inspection-based or audit-based approaches based on 'guidelines' for integrated systems as opposed to defined technical requirements and standards.

The relative weight that may be attributed to the above 'considerations' is to a large extent a 'political choice' that is beyond the scope of this Report to determine.

As part of the study various stakeholders have been consulted as to which specific security products and technologies can be identified as priorities for possible EU-level policy intervention, but opinions on the issue are limited and without any general consensus:

- **For Type 1 products**, a starting point may be to start with security alarm and hold-up alarm systems (for which there is already a private/industry led scheme; CertAlarm) that may be extended to other categories of security electronics products for which European Standards exist (e.g. sensors, control panels) and towards other forms of perimeter and surveillance equipment (e.g. security CCTV systems);
- **For Type 2 products**, a similar approach of building on existing schemes/procedures would bring in products where EU performance requirements already exist (e.g. airport scanners, biometric identity documents). In the case of scanners, this may be extended towards cargo and container scanners which would be relevant for both the aviation and maritime sectors and would have wider application in terms of supply chain security in general. Another area that has been mentioned is eGate type solutions for border control management, which could also have possible applications beyond the aviation sector. However, it remains uncertain at this time as to whether there will be wider deployment of eGate type solutions in the future and, therefore, whether a specific EU CAC scheme would be worthwhile. However, a broader based EU CAC scheme could be considered that would cover biometric based access control systems employed in a variety of security context.

In general, the limited identification of priority products / technologies suggests that there remains a need for greater monitoring of EU markets for security products and of developments in security products and technologies. It may be appropriate therefore for the European Commission to set up or support a monitoring scheme/methodology, which could include also consultation with stakeholders representing both the supply and demand side and authorities with security responsibilities. This could serve to identify those areas where standards and CAC requirements are most pressing.

1.8 Identification and assessment of potential impacts of possible EU-level initiatives to enhance conformity assessment and certification of security products

The nature and character of the security sector has proved to be a strong limiting factor for the quantification of potential impacts, and sometimes even in qualification of the analysed policy options. From both the supply-side and demand-side there is hesitancy to provide information that may be deemed sensitive from a security perspective. Furthermore, information may also be commercially sensitive in so far as it relates, for example, to the cost structures of suppliers of security products. It should also be noted that costs associated to conformity assessment procedures (e.g. fees for product testing) are typically negotiated between the product supplier and providers of conformity assessment services. Quantification of potential impacts is further hampered by the absence of available information on the volume of CAC activities currently undertaken within the EU. This is being the case, the analysis is restricted to a mainly qualitative assessment of potential impacts.

To summarise the potential impacts of EU-level policy initiatives, the following provides a generic description of the main identified impacts – relative to the Baseline Scenario – associated to Option 2 (as outlined above). For Option 3, the impacts should be similar but generally larger in magnitude. It is, however, the case that Option 3 is considered to be considerably less feasible from a technical and political perspective than Option 2.

1.8.1 Impacts on producers

Reduction of costs associated to multiple testing to obtain national certification

Under an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU, security products will have to be certified only once, instead of multiple times. This implies a reduction of costs associated to multiple conformity assessment (i.e. testing) and certification for those products, and in those markets, that are currently required to undergo national conformity assessment and certification. A global estimate of the potential impact in terms of cost savings for intruder alarm systems amounts to a range of EUR 4.7 million to 9.9 million per year.

It can be noted that formal systems for conformity assessment and certification of Type 2 products are relatively poorly developed and cover a limited number of product categories (e.g. screening equipment for the aviation sector, biometric passports) for which some partial solutions exist for EU-wide conformity assessment (testing) of products. For other product categories for which national authorities require some form of approval, the evaluation of product performance is more often organised on an *ad hoc* basis involving a mixture of testing and operational trials. A global estimate of the potential impact in terms of cost savings for airport scanner and screening equipment amounts to approximately EUR 19 million per year.

Additional costs of obtaining EU certification

For products that are currently not covered by national conformity assessment and certification requirements but that will be brought within a future EU-wide system, there may be an additional cost for obtaining certification. Even if certification is not made mandatory, there may still be a development towards a situation where the market requires products to be certified and, consequently, certification becomes a *de facto* obligation. Alternatively, based on a commercial decision, suppliers may voluntarily choose to obtain certification a means to provide an independent verification of the 'quality' of their product so as to distinguish them on the market.

It can be noted that certification is currently not required for most Type 2 products. Accordingly, the development of an EU framework that sets requirements for such products implies that producers will incur the corresponding costs of conformity assessment and certification of compliance with EU requirements. At the same time, as noted above, currently some form of national approval is often applied to Type 2 products. Accordingly the costs of conformity assessment and certification of compliance with EU requirements should be set against the costs associated to existing *ad hoc* approval mechanisms.

Reduction of the need for product trials (Type-2 products)

Type-2 products are often characterised by the development and application of new technologies and approaches in reaction to new security threats or aim to enhance security through, for example, automated and integrated systems. Consequently, both public authorities and potential users are particularly concerned to evaluate the performance characteristics of such products (both in terms of 'security' and operational characteristics). Presently, such evaluation is often undertaken through product trials that are typically undertaken *in situ* at the location where the product will eventually be deployed if the trial is successful. These trial periods can last for several months as has been the case, for example, for trial installations of security scanners (a.k.a. body scanners) that are currently being implemented in a number of EU airports.

From a producer perspective, these trials can represent a significant cost burden. The trials imply putting equipment at the disposal of potential clients (and/or authorities) which has not yet been purchased. This implies that producers have incurred the production (and development) costs, which can be substantial, but are able to sell their product only if and when trials are successfully completed. Moreover, in situations in which different clients (or national authorities) require their own product evaluations then this implies that multiple trials may be necessary. More generally, producers are placed in a situation in which public authorities (and/or clients) indicate an interest in having products available to address particular security threats but for which the actual requirements are not clearly specified and the potential market adoption is unclear. This means that there can be a high degree of uncertainty surrounding the potential returns on RTD investments in new security products and technologies.

The definition of common EU requirements and specifications for product performance and an EU-wide scheme for conformity assessment and certification (or approval) should encompass the specification of protocols and procedures for conformity assessment (including product testing and operational trials). Even though such an EU 'package' may still require some form of product trials, the possibility to certify products as being in conformity with EU requirements after an initial trial should reduce the number of trials that products are required to undergo. Specifically, if clients (and/or authorities) have confidence in certification/approval process under and EU-wide scheme then this should remove – or at least reduce – the need for multiple testing/trials. Moreover, an EU 'package' should provide clear indications on the performance criteria to be assessed through testing and product trials and the relevant protocols to be used which, in turn, may reduce the

duration of trial periods. Overall, therefore, an EU-wide CAC system with mutual recognition of certificates should result in cost savings for producers.

Reduction of the 'time to market' of products

Having obtained a recognised EU-wide certificate, products may be introduced into all EU-markets without the delay caused by requirements to obtain national certification. This implies that suppliers are more rapidly able to (potentially) access the whole EU market rather than staggering product launches in accordance with time taken to undergo separate conformity assessment (testing) to obtain national level certification. This may have a number of implications for producers, for example:

- The scale of production can be aligned at the outset to the expected EU market as a whole rather than being conditioned on (uncertain) timing of national certification. This may result in more efficient investment and utilisation of production capacity and economies of scale;
- The risk that competitors are able to 'replicate' new product developments and innovations is reduced. As a new product can be introduced simultaneously throughout the EU market, this limits the possibility that delays resulting from CAC requirement provide competitors with the opportunity to develop and launch their own similar products. Consequently, the potential returns from investments in research and technology development (RTD) are increased.

It can be noted, particularly in relation to Type-2 products, that the conclusion that 'time to market' will be reduced under an EU-wide CAC system with mutual recognition assumes that the time required to define common EU requirements and specifications for product performance and corresponding conformity assessment criteria and protocols does not exceed that currently required by national authorities/clients. Similarly, it assumes that the time required initiating and implementing product testing and product trials is no more than under exiting *ad hoc* national arrangements. In other words, it presumes that a regulatory process (including definition of product requirements and specification) and operation of an EU-wide CAC system can operate at least as efficiently and rapidly as current approaches.

Reduction of adaptation costs to meet national product standards/specifications

Where divergent national product standards and specifications exist within the EU, producers can be required to supply different variants of their products for different markets in order to meet national requirements. This means, for example, that a manufacturer of a specific type of CCTV surveillance camera has to manufacture several variants of the same product so as to meet specific requirements set in national regulations in different Member States. Thus, instead of producing a single product, the producer must meet the additional cost (both in development and production) of adapting products to individual national markets. Introducing an EU-wide system of conformity assessment and certification, based on harmonised European product standards, should remove the need – and hence cost – for products to be adapted to meet differing national standards and specifications.

Reduction of adaptation costs to meet national conformity assessment procedures

Linked to the previous item, it is evident that national conformity assessment procedures and corresponding testing criteria etc. reflect differences in national product standards and specifications. However, it has been indicated by some stakeholders that, notwithstanding differences in standards and specifications, differences in national testing procedures and protocols can also necessitate further adaptation of products. Introducing an EU-wide system of conformity assessment and certification, with common European protocols and testing criteria, should remove the need – and hence cost – for products to be adapted to meet differing national standards and specifications.

Enhanced transparency of performance requirements and standards / specifications (Type-2 products)

For Type-2 products, the EU legislative and CAC 'package' should provide clear definition of product requirements and technical standards/specifications. It should set out the performance criteria to be assessed, together with the relevant protocols and criteria to be applied for conformity assessment (and certification). In particular, critical performance and testing parameters should be established and codified. Although access to such information may obviously need to be restricted, it may overcome some of the problems associated to the lack of transparency that producers face in having information on the criteria they are expected to meet in order to obtain approval/certification of their products. Further, it should reduce the potential for performance criteria to be determined during or as part of product testing and trials (see above). Overall, the codification of performance and testing parameters should enable producers to develop their products according to 'predetermined' criteria rather than criteria developed as part of the assessment / evaluation procedure. In turn, this should reduce uncertainty of product assessment / evaluation outcomes.

Acceleration of development process (Type-2 products)

For Type-2 products, the introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications should facilitate more rapid product development processes. On the one hand, regulations setting out product requirements and technical specifications should provide producers with a clear indication of the performance characteristics that will be necessary to meet regulatory/market needs. This should make it easier for producers to direct their RTD efforts towards meeting these needs and, also, provide greater clarity/certainty that products meeting EU requirements will be adopted by the market. On the other hand, the existence of a CAC infrastructure may also support the development process. For example, testing laboratories may be involved in an earlier stage of product development (i.e. development testing) where the laboratories themselves will have better information on the criteria and protocols that will eventually be applied to final products. Further, they may be involved in pre-certification testing; i.e. providing partial or preliminary product testing in advance of full testing required for product certification.

1.8.2 Impacts on market conditions

Certification as indicator of product performance

Third-party product certification provides independent verification that a product meets the (performance) requirements against which it is certified and, hence, is an 'objective' indicator for product performance or 'quality'. In the case of products that are currently not covered by national conformity assessment and certification requirements, an EU-wide certification scheme enables a supplier to demonstrate to potential customers throughout the EU that its product meets EU performance requirements. In the case of products that are covered by national conformity assessment and certification requirements an EU-wide certification scheme would have a similar effect but may also reduce 'uncertainty' over product performance that can result from differences in the underlying national product and conformity assessment standards and specifications. Accordingly, an EU-wide CAC scheme may provide for greater transparency of certification and, consequently, of product performance throughout the EU. Since products are certified as conforming to common EU-wide performance requirements, this should facilitate market acceptance of products being offered to the market by 'new' suppliers as it may reduce the importance of 'reputation effects' of established companies. Accordingly, it may be of particular importance for smaller companies (including new business start-ups) and to non-local suppliers that are less well known on the market. As such, certification can act to reduce market entry barriers.

Minimum standards as de facto requirement

There exists an inherent risk that setting (minimum) product performance requirements and a corresponding system for conformity assessment and certification leads to a situation in which products certified as complying with the minimum standard becomes the *de facto* market requirement. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or innovative' products, particularly if they are more costly than standard products that comply with minimum requirements. Essentially, this is an issue that concerns the appropriateness of the standards underpinning the conformity assessment and certification system, irrespective of whether these are associated or not to an EU CAC procedure. However, a possible negative impact of an EU-wide system of CAC that provides for mutual recognition of certification throughout the EU is that it reduces the incentive to produce products with performance levels above the EU minimum standards/specifications.

Increased competition in security product markets

Following from the discussion of different impacts on producers outlined above, there are two main mechanisms through which Option 2 will affect competition in the market for security products:

- First, a single EU-wide system of CAC with mutual recognition of certification should result in an increased in market *transparency*. Products will be certified against common European Standards, providing procurers and users with more insight on the relative performance characteristics of products;
- Secondly, a single EU-wide system of CAC with mutual recognition of certification should increase market *openness* (i.e. reduced market access barriers). An EU scheme allows products to be sold more easily to customers in multiple countries than in a system where products are subject to CAC procedures for each Member State.

Both of these mechanisms should reduce fragmentation and increase the level of competition within markets for security products. As noted, existing suppliers will be more easily able to serve different national markets and such effects may be particularly beneficial to SMEs. The EU market would also be more attractive to new entrants: both new business start-ups and non-EU based suppliers. For the latter, a common EU-wide certification scheme may significantly reduce the entry barriers created through different national level CAC requirements. The extent to which non-European producers will seek to enter and/or increase their presence in the European market, will differ between submarkets but can be expected to be most important for more standardised products. Overall, under normal market conditions, increased competition will put downward pressure on the price of security products, which would reduce costs for procurers / users of the products.

Increased competitiveness of European manufacturing industry

In terms of impacts on the competitiveness of European producers, the main identified mechanisms are as follows:

- Increased market openness and transparency should raise competition within the EU market. Essentially, an EU-wide system of CAC with mutual recognition would reduce the extent of protection provided to incumbent suppliers as a result of existing differences in CAC requirements and systems. This increased competition should drive improvements in productivity performance by forcing improvements in production efficiency and/or raise value added (e.g. higher value-added products);
- Improved market access, which increases the size of the potential market for new products, should provide a positive incentive for producers to engage in RTD activities and promote innovation. Essentially, access to a wider market increases the potential returns from such

development and innovation activities. Interviews with stakeholders confirmed that current market fragmentation is a major barrier to innovation;

- Finally, EU certification may support exports of products to markets outside the EU. A single EU certification may engender greater recognition in international markets than the existing multitude of national certification schemes. Thus, EU certification may be more widely recognised as an international 'quality label' and, hence, support the international competitiveness of European producers. It must be recognised however, that non-European producers that obtained the same European certification would benefit in an equal way from this 'quality label'.

1.8.3 Impacts on procurers and users

Lower price for security products

The previous subsections outlined a number of impacts that affect producer costs and prices and that should feed through to the purchase cost of security products:

- First, there is a decrease in conformity assessment and certification costs. In a market with increased competition it may be anticipated that these costs savings are passed on to procurers /users;
- Secondly, increased market openness should promote production efficiencies and scale economies for producers. Again these should reduce costs and lower product prices;
- Thirdly, as described above, increased competition will lead to price reductions that should be to the benefit of the procurers / users.

Increased product choice / availability

A second impact for procurers / users is the possible increase in product choice and availability. This stems from increased market openness, resulting in more suppliers on the market (European and non-European). At the same time, to the extent that a less fragmented EU market promotes RTD and innovation, there should be increased entry into the market of new technologies and innovative solutions.

Enhanced information / transparency on product performance

An EU-wide conformity assessment and certification scheme should increase market transparency and provide potential purchasers with greater information on product performance. Overall, this should contribute to reducing information asymmetries between purchasers and producers. As described above, product certification provides an independent verification of product performance. As such, it provides purchases with additional insight into product performance.

Facilitation of procurement procedures

Linked to the previous point, an EU-wide conformity assessment and certification scheme should facilitate procurement procedures. Procurers – and where relevant regulatory authorities – would be able to include EU standards and an EU certification as a requirement in their contracts. Furthermore, an EU wide scheme with mutual recognition of certification should support greater openness in procurement procedures by making it easier for potential suppliers to demonstrate conformity to EU standards/specifications rather than needing to undergo separate national procedures. This should increase the number of potential suppliers and result in lower prices of products, as argued above. A benefit related to this will be that the quality of tenders received will be better, as offers from suppliers that do not meet the minimum requirements (as represented by EU certification) will automatically be put aside. Interviews with stakeholders confirmed this to be an advantage of the EU certificates for the procurement of security products that they use. Finally, the procurement process for procurers with a presence in multiple European countries is improved. These procurers will now be able to procure EU certified security products for their entire pan-

European company, rather than being required to use different products in different countries depending on whether the product has obtained the necessary national certification.

Reduced uncertainty of compliance with (user) security regulations

As a final point, where procurers/users of security products are subject to regulatory requirements concerning their security arrangements but where these do not specify requirements for specific products/equipment, the utilisation of certified products may support their compliance with legislation. At least, employing products certified as complying with (EU) performance requirement may reduce uncertainty for users concerning the appropriateness of such products.

Reduced of need for client trials (Type-2 products)

For Type-2 products, as described under the impacts for producers a reduction in the number of product trials undertaken by clients (and/or public authorities) is foreseen. Apart from a cost reduction for producers, this will also result in a cost reduction for procurers / users as certification will now provide independent verification that products meet EU performance requirements, and hence user's staff will no longer be tied-up in conducting product trials.

1.8.4 Impacts on conformity assessment and certification bodies and systems

Change in the volume of demand for CAC services

Replacing multiple CAC requirements by a single 'one-stop' EU-wide approach should decrease total number of CAC procedures required for each individual product and, thus, turnover of conformity assessment and certification bodies will decrease. For products that are currently not covered by national CAC requirements and that are brought within the scope of an EU-wide scheme, there will be an increase in the volume of demand for CAC procedures. Due to a shortage on data on current CAC volumes and the fact that demand will depend on the scope of a 'one-stop' EU-wide approach, it is not possible to assess the net effect of these two impacts. Nonetheless, it seems probable that an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU would result in a reduction in the overall demand for CAC services.

Increased competition for the provision of CAC services

For Type-1 products, interviews with stakeholders indicate that currently CAC bodies in the area of security often have a near monopoly position in their respective Member States. This is reflected in large differences across countries in the procedures and requirements of conformity assessment bodies (CABs) and certification bodies (CBs) and, also, in prices and average duration of CAC processes. The introduction of an EU-wide CAC scheme with mutual recognition of certification should remove the controlling position that CAC bodies are able to occupy over their national markets. Producers would have greater flexibility to choose the CAC bodies that they utilise to obtain certification, which should promote competition between CAC bodies. Increased competition may reduce the prices charged for such services and should also raise the 'quality' and professionalism of provided services.

For Type-2 products, it is important to recognise that the scale of the existing infrastructure for testing of Type-2 products is relatively limited within the EU. For example, we note that only four countries within the EU provide laboratory testing under the ECAC CEP and for testing of biometric passport/identity products/equipment. Similarly, there appears to be limited current capacity for undertaking conformity assessment and certification for other categories of security products/technologies that may be brought under the umbrella of an EU CAC system. In principle, a 'one stop' EU system for certification should potentially increase competition for the provision of

CAC services (as for Type-1 products). It is difficult, however, to assess the extent to which this will be realised and how it will impact on the cost and quality of CAC service provision.

Strengthened EU-wide accreditation

For Type-1 products, it is foreseen that there will be EU accreditation of conformity assessment and certification bodies following common rules and requirements for obtaining accreditation. In this way, the independence and integrity of conformity assessment and certification bodies is maintained. There may also be some improvement in overall quality of services as a result of common requirements for accreditation.

For Type-2 products, in order for Member States and other stakeholders to have confidence in an EU CAC system and procedures it will be essential that appropriate checks are made to assure the quality and independence of CAC service providers. This implies a strong emphasis on the accreditation of conformity assessment and certification bodies; this can be expected to be subject to greater critical attention than for Type-1 products. Accordingly, part of the implementation of an EU CAC system for Type-2 products would relate to the development and operation of the infrastructure and procedures for accreditation of conformity assessment (e.g. testing laboratories) and certification bodies. The definition and application of criteria for EU accreditation of CAC service providers should serve to ensure high standards of CAC service provision.

Increase of administrative costs related to the CAC system

For Type-1 products it is foreseen that conformity assessment and certification bodies will be EU accredited, which will result in corresponding (additional) administrative costs. A detailed costs assessment is not feasible but an indication of the types of costs is as follows:

- Accreditation of security conformity assessment bodies (including testing laboratories) and certification bodies: such bodies - whether existing or created at a future date - will need to be accredited to by a National Accreditation Body and notified to the European Commission. This implies that these conformity assessment bodies may incur costs for the accreditation process (streamlining procedures, audits etc.); normally it is to be expected that such costs will be passed on to their customers in their service price;
- National Accreditation Bodies will incur additional costs for the accreditation of the above conformity assessment bodies;
- Additional cost may also be placed on any organisation providing oversight of national level accreditation or, if applicable, oversight of accreditation within sectoral schemes. It is presumed that for Type-1 products such oversight would be provided through the European cooperation for Accreditation (EA), but this does not preclude an alternative arrangement.

For Type-2 products, the introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications requires also the development of a corresponding organisational structure. This implies additional administrative costs.

1.8.5 Impacts on regulators

Conformity with EU standards as a basis for national regulations

The development and introduction of European Standards and an EU-wide CAC scheme may make it easier for national authorities to introduce national regulations setting product requirements aligned to these standards. Regulators will not be required to develop specific requirements/standards but can make reference to European ones. This may be of particular relevance for Type-2 products (i.e. new and complex technologies) where specific technical knowledge and expertise is required for developing technical standards / specifications. And, with a conformity assessment and certification already be in place, regulators have the assurance that it is

possible to demonstrate conformity with such regulations through the deployment of (EU) certified products.

Facilitation of regulations through existence of conformity assessment infrastructure

For countries that do not possess – or are unable or unwilling to develop – a domestic CAC infrastructure for verifying conformity of security products, the existence of an EU-wide system could remove the need to independently develop such an infrastructure. With mutual recognition of certification under an EU-wide scheme, they could rely on the CAC infrastructure available in other Member States, thus removing the need to have in place or create their own infrastructure. As such, this may reduce the associated CAC infrastructure costs from introducing regulatory requirements for security products. In turn, this may speed-up the adoption of regulations as there will be lower cost and shorter delay in meeting the corresponding requirements for a CAC infrastructure/scheme to verify compliance with regulations.

1.8.6 Impacts on society

It is conceptually difficult to measure the impact that the introduction of an EU-wide conformity assessment and certification scheme would have on society as a whole and on the security of persons, businesses etc. This is particularly the case for Type-2 products that address unpredictable security threats. As Type-1 products typically address 'continuous' and relatively predictable security threats, it is to be expected that increasing the performance of security products should raise overall security levels and, correspondingly, reduce the negative impact of security 'failures' on society. However, it is important to recall that the underlying concerns addressed in relation to Type-1 products are primarily related to 'internal market' and 'industrial policy' aspects, rather than (EU) internal security priorities.

In the above context, the following points may be noted:

- An EU-wide CAC system should raise the average security performance characteristics of deployed products by ensuring that all products meet minimum requirements; i.e. products falling below EU minimum requirements will be removed from the market and already deployed products may be replaced by ones meeting EU minimum requirements. However, there may be risks that a EU-wide CAC system may actually have a negative impact on overall security performance if it reduces incentives for the development of products with performance characteristics above EU (minimum) requirements (see above 'Minimum standards as *de facto* requirement');
- An additional important impact stems from the possible reduction of 'time to market' for security products. One of the problems identified with existing procedures for defining and implementing standards and conformity assessment procedures for Type-2 products is that they are often too slow to respond to new threats and to technological developments. To the extent that an EU legislative and CAC 'package' can accelerate the deployment of security products to address new threats (or enhance the performance of products to respond to 'existing' threats) it should have a positive impact on security;
- Notwithstanding the expectation that an EU-wide CAC system would raise the performance characteristics of security products on balance, one should bear in mind that what is important is the overall security system and not just the performance of an individual piece of equipment. The development of an EU-wide CAC system does not remove the fact that security will only be enhanced if the systems (including procedures and processes) are appropriate for the 'subject of protection'. Therefore, CAC for security products does not remove the need to evaluate broader security systems (e.g. *'concepts of operation'*); including whether the products employed within the system are properly integrated and appropriate given the threat/risk assessment.

Part I - Overview

2 Introduction: study contents and scope

2.1 Background

The technical specifications for this study provide the following points of context for the analysis of the regulatory framework applying to the security industry[5] and conformity assessment and certification procedures for security products[6]:

- The Communication on "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations" (COM(2009) 691 final) indicated with regard to the regulatory framework applying in the security sector that: "*ESRIF has underlined that given the fragmentation of the security market, often due to diverging national legislation, a harmonised regulatory framework in specific areas combined with upstream coordination would be advisable. The Commission considers that as a first step, a thorough analysis of the existing regulatory framework is needed*";
- As regards certification / conformity assessment procedures, the same Communication underlined that: "*Based on the requirements of the end-users and the results of research, new technologies and solutions need not only to be validated; they should also be certified and where appropriate standardised, so they can become part of an effective response to security threats. [ ] Meanwhile, the Commission is exploring ways in which the results of relevant research actions could be tested in view of developing future certification / conformity assessment procedures mechanisms. Such mechanisms should aim at certifying that security products and processes are in conformity with relevant standards."*

2.2 Main elements of the study

2.2.1 General framework

The objectives of the study are to provide a snapshot of the regulatory framework for security (see next sub-section) and a detailed overview of the rules and regulations applying to conformity assessment and certification procedures at national and EU level for security products. Combining these elements**, Chapter 4** describes a general (conceptual) framework linking the regulatory environment to conformity assessment and certification.

2.2.2 Regulatory snapshot

The study aims to provide a 'snapshot' of the regulatory framework applying to the security sector at national and EU level with a focus on regulations applying to security products:

- **Chapter 5** provides an overview of the EU-level security-related regulatory environment as it relates to security products in a number of specific domains[7]:

---

5 The technical specifications specify that the "Security industry is understood as encompassing traditional security industry (based around the supply of general security applications such as e.g. physical access control), security-orientated defence industry (based on the utilisation of defence technologies in security applications or through acquisition and conversion of civilian technologies to security applications), as well as new entrants, i.e. mainly companies extending their existing (civilian) technologies to security applications, such as for example IT companies."

6 The technical specifications specify that "Security products is understood as products developed by the security sector for end-users."

7 These domains were agreed in consultation with the Commission services. In this regard, it was agreed that certain areas of regulation should not be covered by the study, notably: public procurement and pre-commercial procurement, criminal law, (third-party) liability.

- Civil aviation, with an emphasis on airport security;
- Maritime, with an emphasis on port security;
- Critical infrastructure protection;
- Customs controls;
- Export controls / public procurement;
- Data protection.

The overview is complemented by a brief analysis of relevant European Court of Justice cases (Section 5.5).

- National regulatory environments applying to the security sector (specifically security products) are assessed in the accompanying national surveys, with an emphasis focus on:
  - Civil aviation (airport security);
  - Maritime (port security);
  - Urban transport (particularly CCTV surveillance);
  - Energy (electricity transmission and distribution);
  - Data protection and privacy.

An analysis of national technical regulations notified under the 98/34 notification procedure (TRIS database) is provided in **Chapter 6**.

The study is required to analyse where national legislation is diverging in such a way that EU level harmonisation may be warranted, as well as where instances of 'overregulation' or 'non-regulation' may create barriers to trade. An assessment of these issues is provided in **Chapter 5**.

2.2.3 Analysis of conformity assessment and certification procedures

The study aims to identify the rules and regulations applying to conformity assessment and certification procedures for security products at national and EU level:

- **Chapter 7** provides an overview of the EU-wide regulatory approach – the so-called New Legislative Framework (NLF) – for marketing products, in so far as it provides a general EU framework for conformity assessment and certification of products.
- **Chapter 8** presents an overview of some existing supra-national schemes providing for conformity assessment and certification of security-related products. While not attempting to be comprehensive, the identified schemes indicate some of the differing approaches that have been adopted to provide conformity assessment and certification (or approval) of security products;
- National regulatory environments related to conformity assessment and certification procedures for security products, together with existing schemes and infrastructures, are described and assessed in the accompanying national surveys. The scope of coverage follows that outlined above (Section 2.2.2);
- **Chapter 9** provides an overview of the regulatory environment and procedures for conformity assessment and certification of security products in the USA. A comparison is made between the US and EU situations.

2.2.4 *Options for enhancing conformity assessment and certification procedures*

The study aims to identify possible EU-level options for enhancing conformity assessment and certification procedure, including to speed-up existing procedures. These options are to be analysed from a policy and impact perspective[8]:

- **Chapter 10** provides a general framework for assessing the conformity assessment and certification needs and requirements for different categories of security products, distinguishing two main product types. This forms the basis for outlining possible policy options for conformity assessment and certification for each type of security product;
- **Chapter 11** provides an analysis of the potential impacts of the aforementioned policy options, concentrating on the economic impacts and positions of major stakeholders.

In the context of conformity assessment and certification needs, the study is required to examine how priority technologies could be identified.[9] An assessment of this issue is provided in **Chapter 10** (Section 10.5).

[8] Note the technical specifications for the study identified a number of policy options to be analysed. Following from the findings of the study and from the responses to the stakeholder consultation undertaken by the European Commission, the options presented in the study do not correspond exactly to those identified in the technical specifications. The revision of options has been agreed following discussions with the European Commission services.

[9] The technical specifications for the study request a first list of such priority technologies to be provided. As discussed in Chapter 1, such a list is not provided.

3 Overview: current situation, key themes and issues, main findings and conclusions

3.1 General Context

This study aims to examine existing frameworks for conformity assessment and certification (CAC) of security products within the EU, with the purpose of identifying and assessing possible EU-level policy options that may be adopted to speed-up and otherwise enhance existing CAC frameworks. The underlying motivation for analysing CAC in relation to security products is the assertion that – in combination with the parallel development of standards and standardisation processes – improved CAC frameworks for security products would *inter alia* contribute to reducing market fragmentation within the EU, promote the development and adoption of new security technologies and, thereby, strengthen the competitiveness of the EU security industry.

The general situation with regard to existing CAC frameworks was outlined in Ecorys (2009) which, while not alone in drawing attention to perceived shortcomings in existing CAC frameworks, identified two main areas of concern[10]:

- **Absence of common certification systems** for security products at a European level and no mechanism of mutual recognition across countries of products certified at a national level;
- **Slow speed of response and adaptation of certification procedures** notably where new security threats require the implementation of new security solutions and technologies. As a consequence technologies may already be out-dated before approval and certification procedures are implemented.

Such concerns point to the potential for EU-wide policy initiatives to improve conformity assessment, testing and certification of security products, by enhancing approvals and certification procedures and infrastructure. A general objective of such initiatives could either be to generate new certification strategies or harmonise existing ones, with the aim of ensuring that CAC frameworks are adequate to meet EU requirements. Moreover, moving to greater mutual recognition between countries, increasing transparency of procedures, and improving the level and quality of interaction between approval and certification bodies could raise the efficiency of the system and support EU security technology development.

While it is possible to broadly characterise the general situation of existing CAC frameworks, moving towards a more detailed assessment is immediately confronted by the wide-range and diversity of types of products, systems and services that fall under the general heading of security products, which encompass products to address 'traditional' and 'new' or 'emerging' security threats. This is particularly evident in the increasing attention to 'informational' and 'communication' security as opposed to more familiar and traditional 'physical' security concerns. Consequently, it is rather difficult to provide a clear picture of the overall environment for CAC in relation to security products. On the one hand, a relatively well defined EU framework exists for selected security equipment categories, for example in the case for screening passengers and their luggage in the aviation sector, if less so for cargo. Otherwise, there appears to be little in the way of well-defined structures for CAC in relation to security equipment employed in other 'high' priority areas for the EU and where CAC systems do exist they appear to be only at a national level. At the other end of

[10] In addition, lack of transparency in procedures utilised at national levels for approvals and certification – specifically in relation to testing procedures and the feedback on test results received by manufacturers – was a further area of concern.

the spectrum, formal procedures for CAC exist for more traditional and more widely-deployed security products (e.g. intrusion alarms, video surveillance, etc.). Even here, however, the national characteristics of existing CAC systems has led to industry (manufacturers and suppliers) efforts to try to develop European-wide alternatives, though with apparently little general acceptance to date. Another area where industry-led initiatives can be identified is in respect of new technologies, though these are orientated more towards interoperability requirements rather than to the actual security performance characteristics of equipment and systems.

After these introductory remarks we will now turn to a discussion of the general regulatory framework before highlighting key findings of our study.

3.2 Regulatory environment

The terms of reference for this study require the analysis of two main themes:

- The general regulatory framework for applying to the security sector at national and EU level with a focus on regulations applying to security products;
- The rules and regulations applying to conformity assessment and certification (CAC) procedures for security products at national and EU level.

Where the scope of the general regulatory framework analysis is not limited to issues related to conformity assessment and certification requirements and procedures, this summary will concentrate mainly on the linkages between regulatory frameworks and other rules relevant to security products and their implications for conformity assessment and certification requirements and procedures.

3.2.1 Regulatory background

Over the past decade governments in the EU and worldwide have redefined their civil-security concepts and developed comprehensive approaches that combine a broad variety of policies, instruments and actions. This development reflects the recognition of the security threats posed by regional crises, natural disasters and threats from non-governmental actors, in particular terrorism and organised crime. Spurred by the 9/11 attacks, and reinforced by the London and Madrid attacks, the terrorist threat provided the main driver for measures and regulations in the field of civil security. However, at an EU-level, the Internal Security Strategy and more importantly the Stockholm Programme of December 2009 provide a much broader framework than terrorism (and organised crime). The EU security model has become a very wide and comprehensive concept taking into consideration risks and threats of any kind that may have an impact on citizens in a wider perspective and create security problems in a broader sense. For example, the Stockholm Programme action plan for 2010-2014 focuses on measures that include improvements in data protection, strengthening cooperation in civil protection, as well as in disaster management and border control. The recent tsunami in Japan and the ensuing crisis at the nuclear plant in Fukushima are likely to refocus attention on this wider concept of civil-security.

In attempting to provide an overall assessment of the regulatory framework applying to the security sector at national and EU level and, specifically, regulations applying to security products a number of important features needs to be borne in mind[11]:

[11] The following list refers mainly to EU-level but many of the points can be applied equally at a national level.

- At an EU-level there is nothing that approaches a common (single) framework that applies to security products and the market for security products as a whole. Rather, there are a multitude of different rules and regulations that have been adopted to cover security concerns related to different sectors and activities, and with different purposes:
  - They may directly reflect overarching security requirements; for example, common minimum security levels for airports and ports, or biometric passport requirements to improve identification of persons);
  - They may concern the interface between security and individual rights and privacy; for example data protection rules regarding the processing and movement of personal data;
  - They may be motivated by (internal) market and competition considerations; for example public procurement regulations;
  - The may relate to 'generic' product requirements (e.g. health and safety).
- Legislation in the area of security is relatively recent, at EU-level and, in many cases national levels. It is mainly threat driven and follows specific events rather than a long term risk/threat assessment and planning;
- EU-level legislation is limited in scale and scope, with relatively few binding legislative acts that have direct implications for the security sector and the supply of (and market for) security products. In general, EU legal instruments contain rather generic provisions that set minimum common requirements for security procedures and only occasionally apply directly to security products;
- Member States retain a degree of flexibility in transposing EU Directives into national law, leaving room for interpretation. Further, national governments typically retain the prerogative to impose more stringent security requirements. Thus, national differences in rules and regulations, which may be well justified on individual country's security threat assessment, can and do contribute to market fragmentation.

3.2.2 *General regulatory environment applying to the security sector*

Aviation (airport) and Maritime (port) security

The international and EU-level regulatory frameworks are quite comprehensive with respect to aviation (airport) and maritime (port) security. In this regard, however, the EU regulatory frameworks have the ambition of ensuring common minimum levels of security, leaving open the possibility for divergent national situations where the security situation of individual Member States warrants more stringent requirements than implied by the EU minimum requirements.

EU regulations for aviation security provide a framework for the definition of detailed technical specifications required for some categories of security equipment (cf. screening equipment for passengers and luggage) and consequently imply the need for corresponding conformity assessment (validation) processes. The regulatory framework does not, however, provide for a common EU conformity assessment and certification/approval scheme. Different national regulations persist, and it remains the case that national authorities may complete EU-defined security equipment 'standards' with specific national requirements; these may relate to security performance *per se* but may also relate to other operational requirements or non-security concerns (e.g. public and workers safety, protection of private and personal data, etc.).

Despite efforts towards a common evaluation processes for security equipment (see Section 8.2, which describes the ECAC CEP[12]) final approval of airport security equipment remains a national decision. The lack of harmonised security technology standards and common criteria for the

[12] European Civil Aviation Conference (ECAC) Common Evaluation Process for security equipment (CEP).

validation of air transport security equipment – and, more broadly, security solutions and services – leaves the market open to fragmentation. However, the struggle to arrive at an agreed approach to the utilisation of security scanners in airports is illustrative for the problems associated with achieving a common EU-wide position and common standards for security equipment; in this case, concerns about the protection of fundamental rights (together with health concerns) reinforced the extent of debate over the appropriateness and conditions of use of such technologies.

Regarding port security, regulation sets requirements for the designation of port security authorities, which responsible for identifying and taking the necessary port security measures. Commission security inspections of port facilities and companies are carried out with assistance from the European Maritime Safety Agency and are conducted by inspectors from the Member States. Although there are currently a large number of new technologies being developed - e.g. for maritime surveillance, specifically vessel tracking, including Advanced Information Systems (AIS) and Long Range Information Tracking (LRIT) - they are at an early stage and current legislation does not require their use and, consequently, there is no common framework for conformity assessment and certification.

Other Critical Infrastructure Protection (electricity and urban transport)

In other areas of critical infrastructure protection – for which the national surveys focus on electricity generation, transmission and distribution and urban transport – there is a much weaker EU-level regulatory framework. Partly this reflects the limitation that EU-level initiatives have been largely limited to 'European' critical infrastructures having a trans-national dimension. Moreover, EU guidelines concerning common terms, approaches, methods and requirements etc. are lacking. Overall, this means that regulatory frameworks are mainly defined at national and sub-national levels (e.g. for federal/regional structures), with implementation obligations often devolved to local-level administrations.

A particular area of concern is the vulnerability of ICT systems – which in themselves can be considered critical infrastructure – associated to critical infrastructures. There is a perception of a real and growing threat of cyber-attacks targeting critical infrastructure IT networks. At the same time the EU market for ICT / cyber-security is wide and unstructured, and in relation to Critical Infrastructure is viewed as insufficient and often fragmented at a national level. A specific illustration is the development of 'smart grids' and 'smart meters' that are designed to give energy providers and customers greater control over power supplies and potentially to specific appliances. There is concern that such systems may be vulnerable to cyber-attacks, raising issues from data protection of billing information to potential attacks on the supply of power itself. While the Commission Communication on Critical Infrastructure Protection[13] represents a step forward, there is still no EU-wide legislation in this area.

In the field of urban transport, there appears to be an equally unstructured and fragmented market with many decisions relating to security being taken at a local level. One area of interest from a security equipment point of view concerns CCTV surveillance in urban transport environment and is illustrative of local-level fragmentation of security markets. On the one hand, there has been progress made over the last years in the development of European Standards (EN) that cover CCTV used for security purposes. However, there seems to be little evidence of the consistent application of these standards at national (or local) level, or in requirements for CCTV systems used in urban transport environments to conform to these EU standards. On the other hand, the utilisation of CCTV, in particular from the perspective of data protection and privacy, is subject to a

[13] COM(2009)149 "Protecting Europe from large scale cyber-attacks and disruption: enhancing preparedness, security and resilience".

wide array of different national regulatory systems. The diversity of legislation combined with the fact that legal frameworks are seen to lag behind rapid technological developments, suggests that efforts towards EU harmonisation may be warranted[14].

Border security

Following the 9/11 attack in 2001, Member States were asked by the Commission to take immediate action to improve document security, resulting in the integration of biometric identifiers in passports and other travel documents. In accordance with international standards, the Commission established additional technical specifications (e.g. additional security features, storage medium and its security, common quality criteria for facial images and fingerprints).

A comparison between the regulatory framework and supporting initiative take to support the development of EU-wide approaches for conformity assessment and certification for biometric passports (and identity cards) and the approach adopted for automated border control systems (see the two boxes below) provides some interesting insights into the contribution they can make towards overcoming potential market fragmentation.

Biometric identity cards

Based on an international agreement EU Regulation 2252/2004 requires the introduction of biometric identity cards, which can be read electronically across all EU countries. Using an international technical standard developed by ICAO the EU developed an EU particular norm specifying the type of biometry, chip and the functionality required. It also recommended using certification. Tests and certification are carried out on the basis of ISO scheme 15408 with common criteria for the tests.[15] There are only four government test centres that test and certify the equipment in the EU such as the BSI in Germany or ANSSI in France with similar centres in the UK and the Netherlands.

In addition, the Commission together with the Joint Research Centre (JRC) facilitated from 2004 to 2006 several interoperability tests in Paris, Berlin, Brussels and Prague respectively where all identity card manufacturers were tested against suppliers of reading equipment. At the request of DG HOME this activity will be continued for 2nd generation e-passports and electronic residence permits. As a result, while ensuring interoperability, Member States are able to choose what kind of security certification they demand in excess of the European norm. For example, the UK requires not only hardware certification but also a certification that the chip, the operating system (OS) and the entire pass to conform to its standards.

This model is the 'best-practice' according to stakeholders interviewed for this study. It comprises of:

- A worldwide (basic) standard;
- EU regulation;
- EU certification scheme;
- EU facilitation of the process and events to bring together all suppliers along the security value chain at several points in time.

Automated border control

The case of automated border controls illustrates a third way of EU involvement of addressing 'disruptive' security challenges. In this case the original initiative to address the issue did not come from governments but rather from (private) companies. After the authorities had agreed to open up the security function of

---

[14] See, for example, Laurent Lim (2010) "*The legislative framework of video surveillance in Europe*" in European Forum for Urban Security, "*Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV*".

[15] The norm prescribes, for example, which attacks are to be tested, how stable does the chip have to be against a particular threat. This test has been modeled by a security profile (light, electricity, magnetics) and the product needs to be hardened against it.

border control (passport control) to be automated (quasi) private companies drove the process in very different directions without much consideration for issues of standardisation and conformity assessment.

Currently, there are four automated border control projects in the EU:

a. The 'Iris' programme in Heathrow, UK;
b. The 'Mysense' project in Schiphol, the Netherlands;
c. The HBG at Fraport, Germany;
d. The 'Pegase' programme in CDG, France.

Every project has its own requirements, standards and time lines. Importantly, interoperability is not asked for, since automated border control is considered as a strategy to achieve a competitive advantage. Airports (case (a) to (c)) or airlines (Air France in case (d)) want to become more attractive, especially for frequent travellers and, hence, sponsor the implementation of eGates. In order to finance the introduction of the new infrastructure, they make travellers buy a token, valid for one year, which can only be used in one but not any other airport (by passengers of any other Airline than Air France in the case of (d). While the advantage of participating in an eGate scheme might be limited for travellers, the disadvantages for industry are considerable, as singular solutions by different suppliers are developed for each airport.

In this case there is:

- No EU Regulation but rather voluntary programmes in some airports;
- No EU technical specifications but rather proprietary solutions;
- Often not even published information on the requirements set by the operators of eGates;
- No prescriptions for the need of conformity assessment;
- No facilitating role of the EU. Rather in 2009 and 2010 DG INFSO and FRONTEX respectively started to map the eGate landscape Europe and to identify the type of solutions that had been put in place.

For the security industry the disadvantages arising from this model of addressing 'disruptive' security challenges are clear: different standards and requirements, more time to market, less economies of scale, less marketing cloud ('our products conform to EU requirements and can be adopted by any airport in the EU'), especially in comparison to U.S. companies. In the United States the TSA has decided on one eGate standard for all airports and Canada is likely to follow suit.

The general framework for border security is influenced by patterns of participation of Member States in border security arrangements, notably the Schengen agreement and *acquis*. This can be remarked in relation to participation in the three large scale information technology systems in this area. Ireland and the UK participate in EURODAC (European database of fingerprints), but are only partly involved in SIS II (Schengen Information System), and do not participate in VIS (Visa Information System); Denmark is involved in all three systems but on a specific legal basis. While the legal framework is characterised by a 'variable geometry', it is unclear whether this contributes to fragmentation of the EU market for security products.

Export controls and public procurement

The EU Directive of the procurement of defence and sensitive security supplies, works and services (2009/81/EC) aims to bring public procurement more closely into the Internal Market and to open up national markets to competition. The provisions of the Directive are such that it can be supplied across the entire spectrum of security related public procurement, and it is clearly the intention that this may involve, for example, border protection, police activities and crisis management missions. Currently, Member states are still in the process of transposing the Directive into national legislation and so it remains to be seen to what degree it will open up national security markets to competition. In particular, it is unclear to what extent Member States may apply the various exclusions, which

are particular relevance for 'sensitive' security products. Also to be seen is whether companies bidding for security (and defence) equipment and service contracts will be prepared to challenge Member States (routine) use of Article 346 TFEU (Article 296 TEC) exemptions.

Data protection and privacy

The regulatory environment for data protection in the EU including, as it does, reference *inter alia* to the Charter of Fundamental Rights and the European Convention on Human Rights, is worthy of a separate study. The Data Protection Directive (95/46/EC) provides for protection of individual rights with respect to the processing and free movement of personal data; though defence, public security, state security and the activities of the state in criminal law are outside the scope of the Directive. However, with the abolition of the 'pillar structure' through the adoption of the Lisbon Treaty, the Commission intends to include provisions in a revised Data Protection Directive that will cover police and judicial cooperation in criminal matters.

As with many of the aforementioned EU regulations, the Directive leaves Member States the possibility to go beyond the minimum requirements set by the Directive. While each Member State has codified the Directive into law, the interpretation, exemptions and enforcement vary from state to state. This means that despite the Directive, there is a lack of harmonisation across Member States. Furthermore, verification of conformity of IT (and other) equipment and systems with data protection and privacy requirements remains an important issue. Currently, more needs to be done in order to provide independent verification/certification of the compliance of technologies, products or services with legal requirements for data protection.

Technical regulations related to security

The 98/34 notification procedure is a mechanism through which Member States are obliged to notify the Commission of their draft technical regulations related to products and Information Society services before they are adopted in national law. The analysis of notifications over the last decade contained in the TRIS database (see Chapter 6) identifies relatively few notifications appearing to relate of security products. The majority of notifications are IT security-related technical requirements, with relatively few notifications concerning other security products and with no obvious pattern.

While we cannot exclude the possibility that Member States are simply failing to notify the Commission, the findings suggest limited development of national frameworks for concerning technical requirements/specifications for security products. At the same time, the TRIS database is limited to technical regulations at national level (and 'larger' sub-national authorities[16]) and it may be that regulations are being developed at lower administrative levels or by authorities falling outside the scope of the notification procedures. The absence of TRIS notifications would, however, seem to accord with the general perception that weak (national) regulatory frameworks for many categories of security equipment – and corresponding standards and conformity assessment and approval/certification procedures – contribute to market fragmentation.

3.3 Conformity assessment and certification environment

3.3.1 EU 'generic' approach to conformity assessment and certification the New Legislative Framework

The general EU framework for conformity assessment and certification of products as contained within the New Legislative Framework (NLF), which is described in Chapter 7. To date, the use of

[16] Ibid. footnote 84.

the NLF mainly relates to aspects such as protection of health and safety of products but also including electromagnetic compatibility. Some categories of security-relevant products are, however, covered by the Construction Products Directive/Regulation which follows a NLF approach; however this relates to products that are typically somewhat removed from the types of threats normally associated to major civil-security concerns. Otherwise, security-related requirements for products have not been handled through a NLF approach and the utilisation of the NLF to cover requirements related to security aspects and performance of products (and services) is an issue open to further scrutiny. Nonetheless, in principle at least, the NLF could form the basis for any future regulatory approach used to set *inter alia* performance requirements for security products and technologies.

3.3.2 *Supra-national approaches to conformity assessment and certification in the security domain*

Moving away from 'generic' approaches to conformity assessment and certification, it is important at the outset to note that in most instances current approaches – particularly where they concern supra-national schemes – are in many cases relatively new. Accordingly, their lack of maturity makes it difficult to assess their relative strengths or weaknesses. In addition to actual schemes for conformity assessment and certification, it should also be mentioned that a number of EU supported projects (completed and on-going) have addressed the issue conformity assessment and certification in the area of security. We may note, for example, Bio Testing Europe[17], Staborsec (Standards for Border Security Enhancement)[18], Creatif (Network for Testing Facilities for CBRNE detection equipment)[19].

Advanced/New security equipment

Regulation of the aviation sector and biometric identification are among the clearest examples where legislation sets (performance) requirements for security products (see description above). In both these areas, however, it can be remarked that there is not a complete harmonisation of performance requirements across countries and, consequently, differences in national conformity assessment and approval/certification. Also noticeable is the limited scale of the infrastructure for undertaking testing of these categories of security technologies. There are only four government test centres that test and certify biometric equipment and, under the ECAC CEP, only four test centres where EDS can be assessed and three test centres where LEDS can be assessed. Moreover the test centres concerned are located in essentially the same countries: France, Germany, the Netherlands and the United Kingdom.

With regard to other sectors covered by the study – maritime/ports, urban transport, and other critical infrastructure (e.g. power generation, transmission and diffusion) – most supra-national regulations are pitched in terms of requirements for overall security procedures and processes; for example through requiring the designating of security authorities and requiring the Member States to ensure the appropriate security plans are developed. Typically, such regulations do not set out performance or other technical requirements for security products.

General/Traditional security equipment

As noted earlier, a limited number of security-type equipment (e.g. fire alarm and fire protection equipment) are covered within the scope of the Construction Product Directive/Regulation and,

---

17 http://www.biotestingeurope.eu/ This project aimed to set out the prerequisites for the establishment of testing and certification capabilities on biometric components and systems in Europe.

18 http://sta.jrc.ec.europa.eu/index.php/prima-action/60-staborsec Deliverable D5.1 contains a list of existing certification procedures for border security standards.

19 http://www.creatif-network.eu/home.html.

thus, fall with the provisions for mutual recognition of certificates of compliance with EU regulations. Otherwise, for what may be termed 'traditional' security equipment (e.g. intruder alarms, access control, CCTV surveillance, etc.), the EU market is characterised by national schemes for conformity assessment and certification. Where certification is required – and such requirements are by no means common across Member States – suppliers must usually submit to local conformity assessment and certification procedures. There has been very little progress towards common certification schemes and/or mutual recognition of certificates (see also Section 3.3.3). The CertAlarm scheme (see Section 8.3), which has the ambition to provide an alternative EU-wide certificate for 'traditional' security equipment has only recently started (its first certificates were issued in May 2010) and, consequently, it is too early to assess how the scheme will develop.

IT security and data protection

The development of common and supra-national approaches to conformity assessment and certification is often a reflection of the presence of a multitude of differing national approaches. For example, the Common Criteria for Information Technology Security Evaluation - Common Criteria (CC) for short - are the outcome of the efforts of number of governments (USA, Canada, UK, France, Germany and the Netherlands) to develop harmonised security criteria for IT products. However, the CC are seen by some to be too slow and too bureaucratic to respond to rapidly changing developments in information security technologies; in part because they rely on consensus for the development of new standards. It appears that there is some slippage in the use of CC evaluation procedures with certain countries pushing their own national testing regimes.

3.3.3 Insurance-related frameworks for conformity assessment and certification

Moving away from the regulatory environment, the insurance industry has historically an important influence on the development of conformity assessment and certification requirements for security products. This is most evident in relation to 'traditional' security products for which the insurance industry has fostered the use of development of standards for safety and security products. In turn, this has been accompanied by the development of corresponding (national-level) conformity assessment and certification procedures.

In the not so distant past, many aspects of security – comprising the areas of safety and security – have not been specific subject of direct governmental regulation. Originally, it was insurance companies that fostered the use of certain safety standards for objects they insured. This allowed for a reduction and better assessment of risks. The utilisation of certified safety and security equipment has in many cases become a condition for an insurance company to underwrite a policy at all and to set the price. While the scope of security equipment and technologies covered by this kind of certification does not accord with some of the 'high-level' security threats and environments that are identified as priorities from an EU-level perspective, the role of the insurance sector nonetheless warrants attention for several reasons:

- There are sources of standards and for conformity assessment and certification of security products outside regulations. They follow an own dynamic and involve different actors, notably insurance and re-insurance companies. These actors play an important role wherever a security hazard can be translated into a risk, which in turn can be priced;
- The development of some standards and certification schemes might require or might purposefully use the dynamics created by the interaction of private market participants (insurance and re-insurance companies and "their" certifying bodies) to provide for a quick and adequate reaction to technological innovations;
- Insurance companies and "their" certifying bodies represent important stakeholders for CAC in the security sector. At national level, the latter have devised – independently or in collaboration

with national standards authorities – numerous standards and hold a firm hand on their domestic certification market.

One major issue with regard to the role of the insurance sector in relation to CAC or security products is that existing frameworks are essentially nationally organised, with little mutual recognition of certificates between countries. Certifying bodies linked to the insurance sector have been slow to embrace EU-wide solutions, a development that has only started recently. One reason is that national regulations typically make reference to national rather than to EU standards and in some cases EU standards do not exist or they are less stringent than national standards. Furthermore, to some extent it appears that in the past the security industry has at least tacitly accepted the dominance of national certification bodies, as it provided a degree of support for domestic security products in home markets and also in export markets where the label of the certification body was widely recognised as a mark of quality. The entrenched position of national certification bodies would, therefore, be an obstacle to overcome in any initiative towards an EU-wide system for CAC.

A more fundamental issue perhaps relates to the interrelationship between risk assessment and the development of performance standards for security equipment. Insurance companies are able to establish risk profiles that draw on past experience and are able to pool of insurance premiums across insured risks, with recourse to the reinsurance market. This implies that for 'traditional' security threats the risk reduction associated to the utilisation of security equipment conforming to particular performance requirements/standards can be evaluated against potential (financial) losses. What may be the implications that can be drawn from standardisation and CAC in this area, in relation to 'new' security threats (e.g. terrorism) is uncertain.

While the above discussion relates to the use of approved/certified security products, a further dimension to the interrelationship between CAC and insurance is concerned with the supply of products and the liability of the providers of security equipment in the event of a security incident. A particular issue is the third-party liability of security equipment (and service) providers. There appears to be a high degree of concern on the side of industry that present rules within the EU leave it exposed to potentially unlimited third-party liability in the event of a major security incident. Moreover, it is claimed that the insurance market does not currently provide industries with comprehensive options or solutions to meet such exposure. In a recent joint proposal ASD/EOS (2011)[20] argue for EU legislation to places a cap on liability of providers of security equipment/technologies and services (that are alleged to have failed) in the event of terrorist incident. ASD/EOS propose that this legislation should only apply to those services and equipment/technologies that meet set criteria for quality and efficacy. This presupposes, therefore, a mechanism for defining these criteria and for validating that the service or equipment/technology meets the criteria. At the same time, by explicitly linking such a mechanism to liability insurance, it may be reasonable to suggest that this may result in greater involvement of the insurance industry with regard to the specification of requirements for 'approved' services and equipment/technologies and their associated CAC systems.

[20] Joint ASD/EOS proposal on EU Third Party Liability Limitation.

3.4 Key themes and topics

Based on our analysis and engagement with stakeholders, this sub-section outlines some of the key themes and topics that have been identified concerning the regulatory and general environment for conformity assessment and certification in the security sector.

National specificities versus common approaches

While there may be broad agreement at an EU-level on the general nature, scope and perceived magnitude of the main civil-security threats, when considered from a specific local or sector context these can translate in to more heterogeneous security situations and corresponding requirements. Given differences in national (and local) situations, security challenges, and preoccupations, there are strong grounds for arguing that ultimately the evaluation of security threats can only be undertaken at a national level; a position that is reflected in EU legislation (e.g. provisions for Member States to impose stricter security requirements where deemed necessary). This, however, reduces the possibilities to develop and 'impose' EU-wide standards and CAC requirements in so far as they relate to the 'security' and certain 'operational' characteristics of products, as opposed to other aspects such as interoperability requirements.[21]

Administrative and regulatory responsibilities

The rules and regulations setting the conditions of supply and utilisation of products in relation to civil security are determined at different administrative levels from supra-national, via national and regional, down to very local levels (e.g. municipal authorities). While it is the case that international (including EU) frameworks for civil security exist in certain sectors (e.g. aviation and maritime), often many responsibilities for civil security remain at a national-level and are even further devolved to regional and local levels. There is an obvious logic behind the argument that local actors may be better placed to evaluate security conditions and requirements. However, this implies that the prescription of security needs and the corresponding conditions to apply and utilise security products are in many instances set by local actors. Therefore, fragmentation of markets within the EU is not simply a question of differences in national regulations, rules and requirements but of fragmentation within national markets, also.

Market organisation and institutional arrangements

The security market embraces a range from primarily institutional market segments – reflecting public sector responsibilities for civil security – through to essentially private sector market segments. In the middle of this range is something of a grey area where boundaries between public and private sector responsibilities can be blurred. This is particularly evident in respect of several key infrastructure segments that have been characterised by a transfer from public to private sector ownership and operator responsibilities. Approaches to the privatisation trend differ across countries and consequently patterns of public ownership and regulatory and operational responsibility often differ significantly across Member States and even at sub-national levels.

In general, the transfer from public to private ownership implies that, where in the past a single entity (i.e. the government or a government agency) was responsible both for the determination of security requirements and their implementation, these functions are now separated; i.e. an administrative/regulatory authority prescribes security requirements, while the infrastructure operator(s) and service provider(s) are responsible for the implementation of security measures. In an environment in which operators are subject to competition and shareholders' scrutiny of their

[21] In this regard, the EU regulation for of LAG (liquid, aerosol and gel) screening equipment which requires mutual recognition of equipment approved in one Member State by other Member States is a counter example but, also, a development that is of concern to some countries/stakeholders.

performance, this separation can create conflicts in terms of who should meet the financial implications of security; as has been seen, for example, with respect to airport security. Moreover, the break-up of traditionally integrated infrastructure and service providers into multiple operators can in itself result in fragmentation of the market, particularly where there is a lack of coordination of security approaches and functions between different entities.

Public versus private-sector led initiatives

There is a tendency to focus on the role of public authorities and regulatory requirements as the key driver of security markets; this reflects the ultimate responsibility of public authorities for ensuring civil-security, particularly with regard to key challenges such as terrorism, organised crime and disaster management. This position that has been arguably reinforced by the 'privatisation' trend noted above, has resulted in relevant authorities to specify (regulatory) frameworks for security to be observed by private operators. In general, however, public authorities have tended to focus on overall requirements for security which, in turn, has increased attention of standardisation issues, notably in relation to emerging security technology. By contrast, with exception of initiatives in the area of IT security and for specific product categories (e.g. airport scanners, e-passports), conformity assessment and certification issues in these areas have generally received little attention from public authorities.

From a historical perspective, much of the drive for development of standards and conformity assessment and certification procedures for 'traditional' security products has come from the insurance sector. While the preoccupations here are less associated to EU 'priority' security challenges (e.g. terrorism), they are nonetheless relevant in terms of influencing standards and third-party certification requirements for many categories of security equipment (e.g. intruder alarms, access control systems, surveillance systems).

In addition to the above, there can also be a drive from the supply-side, particularly where new technologies require the development of standards and associated conformity procedures in relation to interoperability requirements. What distinguishes such initiatives is that there tends to be less attention to independent (third-party) conformity assessment and certification and more attention to self-declaration of conformity to industry standards and compliance to codes of practice.

Product-based regulation versus obligations and conditions of use for security products

The regulatory framework relevant for security products can be based on differing approaches:

- **Product (supply) based.** Legislation may apply directly to a certain category of security product, setting out 'blanket' conditions (e.g. minimum technical specifications) to which the products must conform in order to be made available on the market; this is the case, for example, for generic 'health and safety' requirements. Typically, some form of product testing is required to verify compliance with such '*product-based*' legislation[22];
- **Sector (demand) based.** Legislation may apply to the customers and end-users of security products; for example where security requirements are set for specific economic sectors or activities[23]. Such regulations are limited to setting obligations on the relevant 'actors' – either public or private sector, or both – to ensure adequate measures are implemented to maintain security; for example, as is the case for port security. Typically, compliance with such '*sector-based*' legislation is based on inspection and auditing of security procedures of conformity-

[22] Such legislation can specify the applicable mechanisms for determining conformity with the requirements, including by whom the activity is performed (e.g. manufacturer, user, independent conformity assessment body) and the form in which the declaration of conformity is made (e.g. self-declaration, third-party certification).

[23] This may also include legislation and regulations relating to public procurement.

assessment. However, the technical requirements associated to particular categories of security products which may be utilised to achieve compliance, are not themselves specified;

- **Hybrid 'sector-product' based.** A 'hybrid' of these approaches is provided where legislation not only sets out obligations to fulfil certain security functions, but also sets out the relevant means (and technical specifications thereof) through which the security function is to be performed. This is the case, for example, in passenger and luggage screening in the aviation sector.

To date, the main thrust of security-related regulations has been of the second type listed above. Security regulations are typically orientated towards a particular type of (economic) environment (e.g. aviation, maritime, critical infrastructure, etc.) or activity (e.g. border control, management and transport of hazardous materials, etc.). As such regulations do not directly provide technical specifications for security products, leaving the evaluation of the appropriateness of employed products/technologies to the discretion of the relevant authority or inspectorate. Further, this leaves open the possibility that other instruments – e.g. administrative circulars and guidelines, advice notes, codes of practice, voluntary agreements – that recommend the use of given specifications or standards, can set compliance requirement that though not mandatory can become *de facto* obligatory.

Confidence in CAC frameworks

Any efforts towards common EU approaches for CAC must be able to guarantee confidence in the 'quality' and 'independence' of approvals and certification outcomes. In particular, this relies on the strength of mechanisms for accreditation of conformity assessment bodies and, in particular, test laboratories (and other similar organisations) responsible for verifying conformity. In this regard, the limited number of suitably qualified testing laboratories (e.g. there are only four laboratories associated to the ECAC CEP) suggests that there may be capacity constraints with existing CAC infrastructure.

Standards and CAC for single equipment versus systems

Existing performance standards and corresponding CAC arrangements are at the level of individual equipment and components. Many stakeholders point to the need for systems approaches that look at systems that combine different equipment (e.g. complex checkpoint solutions) and that also take into account the provision of services that are directly linked to products/equipment. Conformity of individual products/equipment does not ensure the effective provision of security. Individual products/equipment need to be able to 'communicate' and 'collaborate' with other products/equipment in the system; and the system often has to be connected to service personnel (e.g. security service providers, police) to provide effective security protection and response.

Certification of products versus certification of systems

Following from the above point, addressing conformity assessment and certification requirements for complex systems raises issues related to which of the parties are positioned to obtain approval/certification. For individual products it is evidently possible for the manufacturer/supplier to obtain approval/certification of their product. However, when dealing with large systems that integrate equipment from different suppliers and/or where the configuration and operational characteristics are specific to the particular environment in which the system is deployed, either the system integrator (where there is one) or the actual operator will need to obtain approval/ certification of the system. In this regard, given that large systems are more closely linked to the environment in which they are deployed then it is probably more difficult to harmonise certification of systems, than it is to harmonise certification at the individual product level.

Regulatory barriers to the introduction of new equipment

The EU regulatory framework which defined a list of eligible methods and technologies for passenger screening, is a case in point. Airports are not permitted to replace systematically any of the recognized screening methods with security scanners before this is added to the legally binding list of eligible methods. This framework presented a barrier to the introduction of LAG (liquid, aerosol and gel) screening and security scanners ('body scanners'). This implies that the aviation security market, and in particular the security scanners market is restricted within the EU and that current legislation hinders its full functioning.

Privacy and data protection issues

The on-going debate over the use of security scanners highlights the role of 'ethical' issues such as privacy and data protection. In the absence of a clear European framework in this area and at national levels also, there is an absence of clear guidelines for equipment/technology providers with respect to accepted and acceptable performance requirements. A similar situation exists with respect to protection of personal data collected and held by biometric identification systems, for which national approaches and requirements vary significantly.

Limited involvement of end users and other stakeholders in the elaboration of standards

While there is an underlying principle that standards should be developed on a 'consensus' basis, in many areas there appears to be little involvement of end-users. Standardisation bodies, certification bodies, technical experts (that may themselves be part of the CAC infrastructure) and other stakeholders such as the insurance industry tend to comprise the main participants in the development of standards, with lower representation of end-users.

Certification not appropriate for all conformity assessment issues in the security sector

As mentioned above, conformity assessment in the security sector is sometimes done on the basis of a classified 'standard', as for example in the case of security plans for ports or airports or the performance criteria in case of some ECAC tests. Here the classified character of the 'standard' contributes to the security function. In these cases the integrity of the conformity assessment processes is of critical performance and may limit the scope for assessments to be conducted by private certifying bodies for two reasons: this would increase the number of people who would require access to the information; and certifying bodies are often private companies operating in a market and their incentive structures might lead to a conflict of interests to the task they have to carry out. Both aspects do not only increase the risk but also call for additional checks on the reliability of the certifying bodies.

EU level lead for newly developed equipment

For a number of cases where security functions were opened up to automation (for example in the case of eGates at airports, biometric passports or electronic tachometers) or new technology had to be developed to address new threats (security scanners, liquid explosive device control). In these cases EU level leadership promises to ensure that a single market across the EU rather than a number of national markets emerge. While private actors such as airports, airlines (or in the future ferry companies and ports) might want to seek a competitive advantage and therefore lead the introduction of such new technologies, early EU action is required in each new case as to ensure one level of security across the EU and to avoid market fragmentation.

4 General framework linking security regulation, conformity assessment and certification

4.1 Introduction

This Chapter sets out a general framework linking (security) regulation, conformity assessment and certification.

4.2 Main elements of the general framework

Figure 4.1 provides a general schematic framework linking the main elements of the study:

- The **regulatory framework** is *inter alia* concerned with legislation (laws) and accompanying regulations that specify requirements to be fulfilled in order to be in compliance with the legislation. Such regulations[24] – notably 'technical regulations' – may themselves set out the specific requirements to be fulfilled, or make reference to other normative documents, such as standards, technical specifications, codes of practice etc.[25]
  While it is normal to think of the regulatory framework with reference to specific requirements in relation to the supply of 'products'[26], in the context of the security sector specific requirements may equally be imposed on the procurer or user (of security 'products'); for example, legislation/regulations may specify that a particular category of user can only utilise security 'products' meeting specified requirements. Alternatively, a user may be required to implement security procedures and systems that – explicitly or implicitly – impose specific requirements on the security 'products' utilised;
- **Specified requirement** is a general term to denote a stated need or expectation that should be fulfilled by the *object* (of conformity assessment). Specified requirements may be stated in normative documents such as *regulations*, *technical specifications* or *standards*. More broadly specific requirements may be covered by conventions, codes of practice etc. established, for example, by a professional or industry association or at the level of a specific company (e.g. corporate 'standard'). In this regard, the following sources may be noted:
  - ***Technical Regulation:*** a regulation providing technical requirements either directly or by reference to *inter alia* a standard, technical specification or code of practice. A technical regulation may be supplemented by technical guidance that outlines means of compliance with the requirement;
  - ***Technical specification:*** a document that prescribes technical requirements to be fulfilled by a product, process, system etc.[27] A technical specification may be a standard, a part of a standard or independent of a standard;
  - ***Standard:*** a document that provides for common and repeatable use, rules, guidelines or characteristics for activities or their results. A standard is **established by consensus**[28] -

---

[24] In a general context, regulation may apply more broadly than rules and restrictions resulting from legislations. For example, self-regulation by industry/professional associations.

[25] Where this is the case, compliance with otherwise voluntary standards, codes of practice etc. may become mandatory.

[26] In this sub-section the term 'products' is used in its most general sense and should be understood to refer to products, services, processes, systems, persons, bodies or other relevant items or activities.

[27] This is in general accordance with the definition provided in under the New Legislative Framework (Decision No 768/2008/EC.). It may be noted, however, that the definition therein refers to a product, process or service.

though not necessarily unanimity – and agreed upon through a formal process; hence, providing the legitimacy and authority of the standard;

- ***Code of practice:*** a document that recommends practices or procedures for the design, manufacture, installation, maintenance or utilisation of equipment, structures or products. A code of practice may be a standard, a part of a standard or independent of a standard.

As noted above, specific requirements and their relevant standards may be identified by regulations. In addition, specific requirements may result from non-regulatory mechanisms. This may be the case where, for example, specific requirements are prescribed (for example, under a standard or code of practice) by an industry, trade or professional association. Typically this relates to suppliers but may also reflect requirements that are specified by – or imposed upon – procurers/users.

Following from the above, the term 'specified requirement' is understood to refer only to those requirements that can – actually or potentially – be established with reference to a normative document or some other form of recognised rule or procedure (e.g. a code of practice), or by convention. Consequently, determination of the fulfilment of a specified requirement must be possible – actually or potentially – through a conformity assessment scheme or procedure. Other requirements that may be specified in relation to a security 'product', for example contractual specifications between a supplier and procurer/user of a security 'product' that are essentially unique to an individual contract are not considered to fall within the definition of a specified requirement.

Note: While it evident that standards and conformity assessment/certification are inherently linked, it is not the purpose of this study to identify or specifically assess standards, standards-procedures or standards requirements in relation to security. For the purposes of the study, standards are regarded as one element of the context determining conformity assessment/certification requirements and procedures. Differences in standards may, for example, be a factor contributing to differences in national-level conformity assessment and certification procedures that, in turn, may warrant some form of EU harmonisation. Similar, lack of appropriate standards may in turn underlie the absence of conformity assessment/certification procedures in areas where there is an evident need for such procedures and, hence, some form of initiative (national or EU-level) may be called for to establish both standards and certification process. However, for the purposes of the study, the focus of attention is on those aspects of regulations, rules and procedures where actions may be warranted to speed-up or otherwise enhance conformity assessment/certification of security products, rather than on the underlying standards and standard-setting processes.

- **Conformity assessment** (programme or scheme) is used to demonstrate that the specified requirements relating to a 'product' are fulfilled[29]. Conformity assessment may be directly required under specific legislation and/or regulations, which may also specify the way in which the conformity assessment is performed (i.e. by whom: manufacturer, user, certification body; and by which method(s): e.g. testing, inspection, audit).
  Depending on the nature of product (or service), process, systems, person or body (hereafter, "*object of conformity assessment*") and the nature of the specified requirements, various methods may be used to determine if the *specified requirements* are fulfilled. Common types of determination activities include:

[28] Consensus implies general agreement characterised by absence of opposition to substantial issues by any important part of the concerned interests. Also, it implies a process to take into account the views of all parties concerned and to reconcile any conflicting arguments.

[29] This is in accordance with the definition provided under the New Legislative Framework (Decision No 768/2008/EC). It may be noted that the term 'specified requirements' is not defined in the Decision.

- ***Testing:*** used when the characteristics can be evaluated via measurement under specified conditions. Testing typically applies to materials, products or processes. Testing procedures commonly take place in accredited testing laboratory facilities;
- ***Inspection:*** used when the critical characteristics can be evaluated via physical examination or measurement. Inspection may cover examination of a product design, product, process (which may include inspection of persons, facilities, technology and methodology) or installation. Inspection may be used to ensure that all parts of a system have been properly installed;
- ***Audit / Registration:*** used to provide an assurance that a process meets requirements. Typically audit / registration (schemes) applies to management systems;
- Conformity assessment can be a discrete activity (i.e. one-off) but, in some cases, on-going activities may be required to ensure the continued determination that specific requirements are fulfilled. Thus a further activity is:
- ***Surveillance:*** consisting of a systematic 'iteration' of conformity assessment activities to maintain the validity of a statement of conformity.

Conformity assessment in the security sector does, in principle, not vary from that in other sectors. There are technical specifications, on the one hand, and 'products' on the other and the conformity of the latter with the specification of the former has to be established. What is different, however, is the more significant role of third party CA (see below) due to the higher risk associated with non-conformity and non-compliance; and the secrecy of some technical requirements set by government bodies. For example, some governments do not publish the minimum mass of explosive that a sensor needs to be capable of detecting to be usable at an airport.

- **Conformity assessment body:** is a body that performs conformity assessment services[30]. Conformity assessment may be undertaken by different parties:
  - ***First-party conformity assessment:*** performed by the person or organisation that provides the *object* (i.e. seller or manufacturer). A statement of conformity issued under a first-party conformity assessment is typically in the form of a Suppliers Declaration (of conformity);
  - ***Second-party conformity assessment:*** performed by a person or organisation that has a user interest in the *object* (i.e. purchaser or user)[31];
  - ***Third-party conformity assessment:*** performed by a person or body that is independent of the person or organisation that provides the object, and is independent of the user's interest in the *object* (e.g. an independent assessment/certification organisation). A statement of conformity issued under a third-party conformity assessment is typically in the form of a Certification (of conformity).

  First, second or third-party conformity assessment systems may be utilised. However, in the context of 'security', for which risks associated to non-compliance are high *a priori*, third-party conformity assessment may generally be required[32].

---

30 This is in accordance with the definition provided under the New Legislative Framework (Decision No 768/2008/EC), which provides the following definition:" 'conformity assessment body' shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection."

31 Unlike first-party (declaration) and third-party (certification), there is no common generic term to describe an attestation/statement of conformity provided by a second-party.

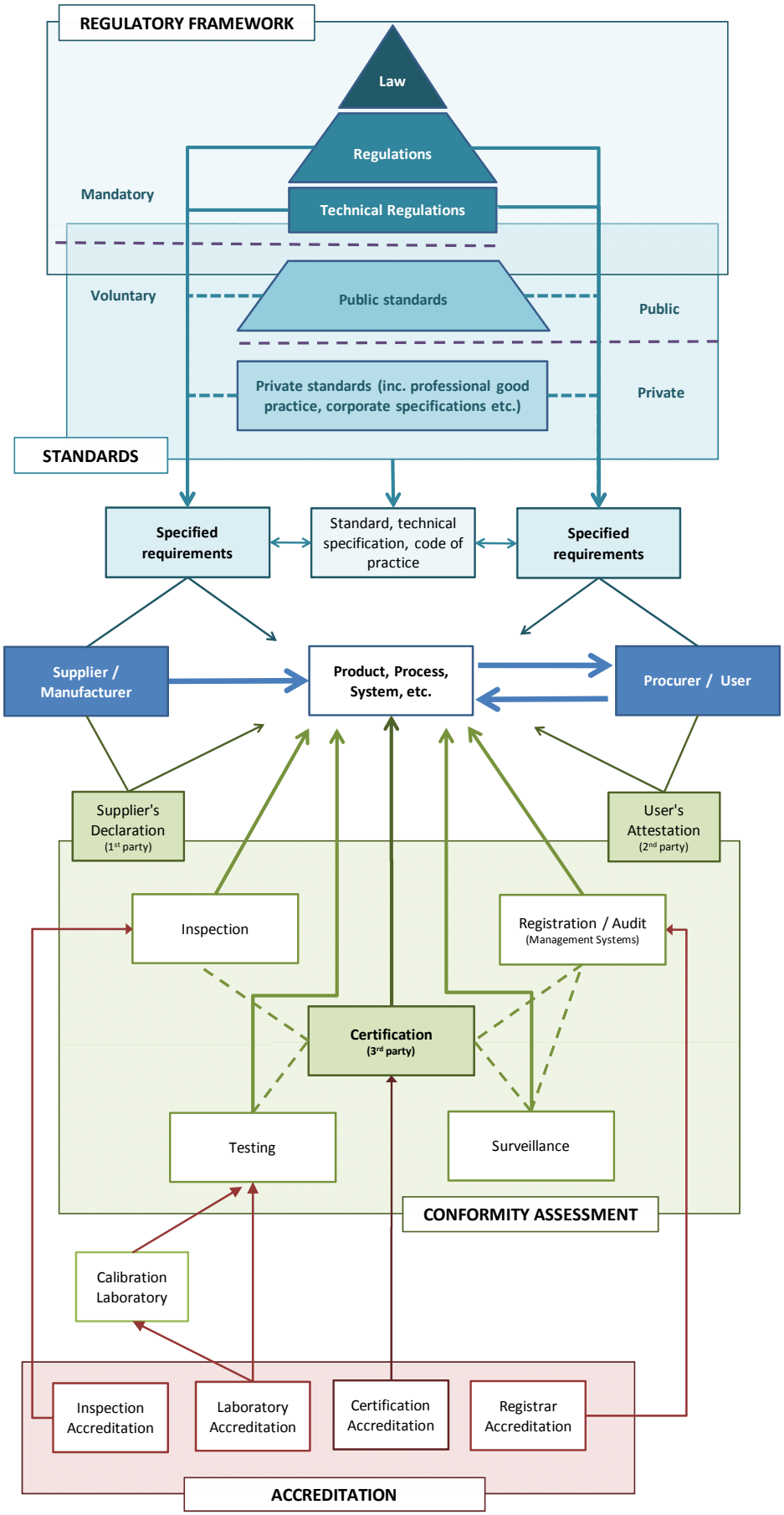
32 See, however, the discussion of which parties may be more closely associated with conformity assessment procedures in Section 4.3.

- **Certification** is a statement/attestation from a third-party (e.g. an independent assessment/ certification organisation) that a 'product' fulfils the specified requirements. From the above, it is only one of three ways in which conformity of an object to specified requirements may be demonstrated. Certification may be required by legislation/regulation. More broadly, certification may be required by users; for example as an assurance that a 'product' is of a required 'quality or 'reliability' (i.e. 'fit for use') and may serve to increase transparency/comparability of products. Similarly, certification may be driven by supply-side considerations, again to raise market transparency and to 'inform' users but, also, to promote fair competition (i.e. that all 'products' sold within a given market should be certified);
- **Accreditation** is a third party attestation (or approval) relating to a conformity assessment body (such as a certification organisation conveying formal demonstration of its competence to carry out specific conformity assessment tasks. It provides a means of assessing and ensuring (or enhancing) the 'quality' of activities of a conformity assessment body (e.g. in terms of management, competences, and technical capabilities). As such, it provides a mechanism for providing confidence in conformity assessment activities (e.g. laboratory testing and results) and, in turn, confidence in certification schemes. The authority of an accreditation body is generally derived from government.

Note: Under the New Legislative Framework, accreditation is given a more specific definition, namely "'accreditation' shall mean an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity". Further, "'national accreditation body' shall mean the sole body in a Member State that performs accreditation with authority derived from the State"[33].

[33] Regulation (EC) No 765/2008. The Regulation also provides that "Member States should not maintain more than one national accreditation body and should ensure that that body is organised in such a way as to safeguard the objectivity and impartiality of its activities. Such national accreditation bodies should operate independently of commercial conformity assessment activities." Further "In order to avoid multiple accreditation, to enhance acceptance and recognition of accreditation certificates and to carry out effective monitoring of accredited conformity assessment bodies, conformity assessment bodies should request accreditation by the national accreditation body of the Member State in which they are established. Nevertheless, it is necessary to ensure that a conformity assessment body is able to request accreditation in another Member State in the event that there is no national accreditation body in its own Member State or where the national accreditation body is not competent to provide the accreditation services requested."

Figure 4.1 General Framework: Security Regulation, Conformity Assessment and Certification



4.3 Linking security products to conformity assessment and certification

This section seeks to relate security products – in terms of their general characteristic and main distinguishing technical and process-related requirements – to potential conformity assessment needs and, in turn, to likely characteristics of associated conformity assessment schemes.

A large number of product categories falls within the general description of 'security products', where this is understood as products developed by the security sector for end users[34]. Even if an equipment-orientated approach is adopted, the array of potential 'products' can stem from basic security equipment such as surveillance cameras, to more complex equipment such as security scanners, beyond which are the systems linking different equipment together and, in turn, systems of systems (SoS) that integrate various (security) systems[35].

In general terms, two dimensions for describing a security 'product' in relation to potential conformity assessment and certification requirement are apparent:

- The first relates to the relevant '*scale*' at which requirements may be specified; for example from micro-level for individual security devices or components to macro-level of broad systems-of-systems;
- The second relates to the '*scope*' of requirements that may be specified; for example, these may be purely technical characteristics of (security) equipment, or may be related to security processes and procedures. Procedures can refer to how certain activities are to be done or how a person, filling a specific position, has to be adequately trained in order to ensure that the security system is working properly.

For example, in the case of airport security, requirements may be set for the technical capabilities of detection equipment for baggage screening or at the level of security processes and procedures to be implemented for an entire airport.

From the above, and notwithstanding the findings of the study, Figure 4.2 illustrates the possible interactions between security 'products', specified requirements and conformity assessment:

- At the lowest level, **security 'products'** may encompass individual components or devices, followed by equipment and sub-systems and moving up through systems and systems of systems. Concerning the latter, it is difficult to develop clear definitions of what constitutes a 'system' or a 'system of systems' as, even within the security domain, the terms are used to cover quite different levels of integration of equipment and systems[36]. What can be noted is that a system-of-systems approach may be related to a specific environment or location (i.e. 'local SoS'), or be applicable across environments or locations (i.e. 'global SoS'[37]); for example we can think of various security systems within an airport as being elements of an overall airport security system-of-systems, while the linking of such systems-of-systems across airports may be part of an overall security system for the aviation sector;
- There may be a wide variety of **technical requirements** that may be specified for different level of security products depending on specific circumstances. However, it seems reasonable to postulate that as security products/systems become more complex and integrated there will be

---

34 This is the definition provided by the European Commission in the technical specifications for the study.

35 ISO/EIC 17000 provides a broad definition of '*object of conformity*' that not only encompasses a product (or service), but also any particular material, installation, process, system, person or body to which conformity assessment is applied.

36 As a general indication, a system-of-systems can be understood as *"large scale integrated systems that are heterogeneous and independently operable on their own, but are networked together for a common goal"*. This description is borrowed from: *System of Systems Engineering: Innovations for the 21st Century*, Edited by Mo Jamshidi, 2009 John Wiley & Sons Inc., Publication.

37 This is not intended to imply global in a geographical sense.

an increased emphasis on requirements relating to aspects of compatibility and interoperability. Conversely, requirements for individual components or equipment are more likely to relate to suitability to perform a specific task(s) and, in this respect, the extent to which components or equipment have similar performance characteristics and are, therefore, interchangeable (i.e. in the sense that another 'product' may be used to fulfil the same requirement);

- Similarly, from the perspective of **process requirements**, it seems reasonable to expect that requirements for higher-level more complex systems are more likely to relate to issues linked to information exchange and communication. Whereas at lower levels there will be more emphasis on requirements that processes and procedures can be replicated (e.g. regular and/or repeated implementation of a specific security task(s));
- From the perspective of **conformity assessment activities**, it can be envisage that testing activities are more likely to provide a means for determining if specified requirements have been fulfilled when they are applied at the level of components, equipment or small scale systems. Not least, this may be the case given that testing procedures can be applied across a multitude of different 'products' that are required to perform the same (or similar) tasks[38]. Inspection activities may be more relevant at a system level, for example to ensure that all elements of a system are compatible and interoperable or that all elements of the systems have been correctly installed. For more complex systems (i.e. systems-of-systems) for which technical and process requirements may themselves be more complex or heterogeneous, the audit-based methods of determination of conformity may be more applicable[39];
- From the perspective of **conformity assessment actors**, it is perhaps also possible to postulate which parties may be more closely associated to conformity assessment procedures depending on the type/level of product concerned. Notwithstanding that there may be specific needs for (independent) third-party conformity assessment – not least if this is required to be in compliance with prevailing regulations – for higher-level, more complex and potentially unique systems, the determination of whether specified requirements are fulfilled is more likely to depend on the evaluation made by the user of the system (i.e. second party assessment) or the evaluation by users of similar systems (e.g. peer review). By contrast, for components, equipment or small scale systems we may expect greater participation of suppliers. This may be either because a statement of conformity may be provided directly by the supplier/manufacturer (first-party conformity assessment)[40] or because, in addition to the possible interests of public authorities, suppliers may have a commercial interest in supporting the application of third-party conformity assessment and certification.

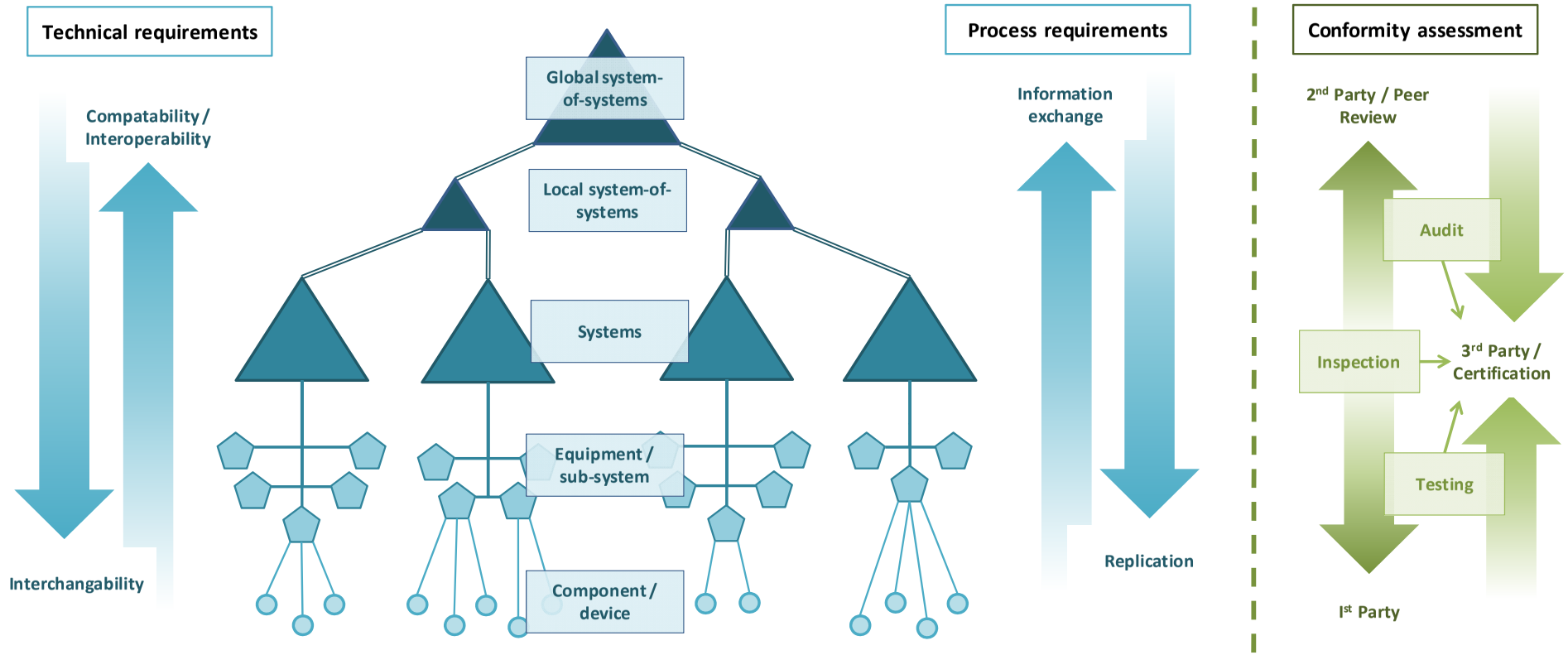
---

[38] Testing (type test) can be carried out, for example, on samples of 'products' to determine conformity.

[39] Higher level systems (systems of systems) may have unique characteristics, hence requiring assessment on the basis of best-practice principles/criteria (e.g. for operational/management procedures) rather than measurement or physical evaluation.

[40] A supplier's declaration is usually only used when risks associated with non-compliance is low. While this is unlikely to be viewed as the case for most security 'products', it may apply to components or devices incorporated in security equipment or systems.

Figure 4.2 Security 'products': specified requirements and conformity assessment



4.4 Security dimensions of conformity assessment and certification

This section seeks to outline the broad dimensions of security-related requirements that might result in specific requirements for security 'products' that may be subject, in turn, to conformity assessment (and certification) procedures.

As a starting point, a distinction may be made between:

- **Generic product requirements** unconnected to the security-related capabilities of (security) 'products'. For example, these may include health and safety related aspects, or for electrical and electronic products requirements related to electro-magnetic compatibility etc. In other words, these are general requirements that need to be complied with irrespective of the security dimension of 'products';
- **Security-specific product requirements** that are directly connected to the security-related capabilities of (security) 'products' or that stem from the utilisation of products in a security context or environment[41].In addition to the above two categories, there may be other requirements that are not necessarily directly connected to the security-related aspects of a 'product' but that are, nonetheless, seen of being closely associated with security 'products'. In this respect, we can think of '*ethical*' or '*societal*' requirements related, for example, to privacy (e.g. body scanners) and data protection concerns (e.g. non-disclosure of personal information). Thus a further category of requirements may be:
- **Associated product requirements** that are connected to general/transversal principles (e.g. ethical / societal / human dimensions) and requirements that, though not specific to security 'products', are of particular relevance or concern in relation to security 'products'.

> **Note:** It is not the purpose of the study to identify and assess conformity assessment/certification rule and procedures in connection with 'generic' product requirements. There is an underlying presumption that security products – as with other products - comply with such requirements.

As noted in the previous sub-section, the scope of security 'products' may encompass anything from an individual device or component to a large integrated security system of systems that delivers – or, at least, brings together and integrates – a wide range of security capabilities. From a parallel perspective, we can also see that the specification of security requirements may vary from the capabilities associated to broad security objectives or missions down to specific technical (performance) requirements associated to individual types of security equipment or activities. In this regard, in identifying and establishing - actual or potential – requirements for conformity assessment (and certification) we can envisage a 'top-down' approach starting from overarching security requirements and working down through system-level and product-level requirements. Alternatively, a 'bottom-up' approach may be used that starts at the level of equipment etc. and move up towards the attainment of overarching security requirements. In general terms we can think of three levels for defining requirements that may be of relevance for security products:

- **Overarching requirements** derived from the main security objective or mission with respect to which the security 'product' may be employed[42];
- **Functional requirements** derived from what 'outputs' need to be provided (or 'inputs' utilised) in order to deliver the security capabilities required to fulfil the security mission;

---

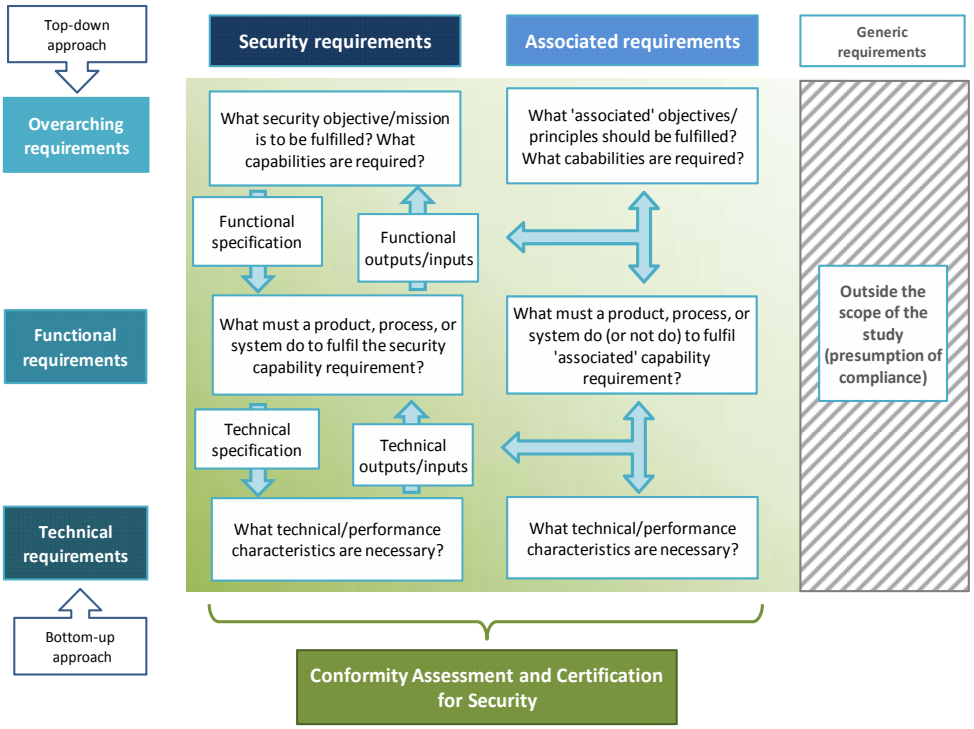
[41] In this regard, it may be noted that some products are intended specifically to be used to provide security-related capabilities. Other products may have a wider utilisation that is not limited to security applications but for which specific (additional) requirements may be applied when they are used to provide security-related capabilities or are used in a security context/environment.

[42] Typically, in a system engineering type context, the top-level would be characterised as the 'business requirement' (i.e. what needs to be achieved).

- **Technical requirements** derived from the technical characteristics (e.g. product performance, interoperability, etc.) that are necessary for a 'product' to contribute to delivery of a security capability.

The aforementioned elements are brought together in Figure 4.3 . From this, certain issues that arise are: the extent to which conformity assessment and certification be applied to security products as (specified) requirements move beyond technical performance and interoperability aspects and towards higher level requirements, and the extent to which conformity assessment and certification jointly address security and non-security related (i.e. associated) requirements.

Figure 4.3 Broad dimensions of security-related requirements



Part II – Regulatory framework snapshot

5 EU security-related regulatory framework

5.1 Introduction

This chapter presents a snapshot of the EU legislative framework applying to the security market. The snapshot is based on a selection of legislative measures which, according to our analysis, may have the highest impact on the development of security-related capabilities and therefore on the supply side of the security market.

Community law is made of Primary Legislation, and Secondary Legislation[43]. The legislative measures selected for the snapshot are the one with binding effects, namely Regulations having general and direct application for all Member States and Directives having application as to the objectives to be achieved by all Member States and after transposition into national law. Any attempt to assess exhaustively the entire regulatory environment, and even more so to analyse the concrete implications of each legislative act for industry, would go beyond the limits of this paper. We will therefore choose a more selective approach and tackle the issue from two different angles:

In a first step we will look at the EU's general policy and strategic framework for security activities. Our objective is to regroup the multitude of regulations across the different security areas addressed by EU policies. We will select areas of high economic importance where we expect a particularly strong impact from regulation on industry, in particular since investments are (potentially) important, namely:

- infrastructure security (aviation, maritime, critical infrastructure) ;
- border security;
- customs security;
- data protection;
- export control;
- procurement rules.

We will then define the main features of these regulations.

In a second step, we will have a closer look at each security area. We will show how political objectives are translated into concrete regulation and how EU and national competences interplay. We will also identify the challenges ahead and the limits of the current EU legislation.

5.2 Context

It is generally recognised that the main security threats today are not large-scale military conflicts, but regional crises, natural disasters and threats from non-governmental actors, in particular terrorism and organised crime. Facing such threats, governments in the EU and worldwide have redefined their security concepts and started to develop a comprehensive approach, combining a broad variety of policies, instruments and actions. This is also the case at EU level. There are a

[43] The Treaties agreed upon by Member States form the EU Primary legislation. They define the role and responsibilities of the various EU institutions and bodies as well as establish the legislative, executive, and judicial powers of the EU. These secondary forms of legislation stem from the Treaties and require both binding and non-binding actions on behalf of the Member States, amongst which: Regulations, Directives:, Decisions (fully-binding EU laws regarding specific cases and are addressed to particular parties), Recommendations: Are “opinions” which are non-binding.

number of key documents which set the framework for EU policies and actions in the security field and guide the launch of regulations in this area, in particular:

- The EU security Strategies: the 2003 Security Strategy[44]complemented in 2010 by the Internal Security Strategy[45];
- The Counter-terrorism Strategy, with the latest update in 2010[46]; and
- The Stockholm Programme adopted in 2009 and the related Action Plan of April 2010.

These policy documents show that after 2001 the terrorist threat was indeed the main driver for measures and regulations in the field of security. The London and Madrid attacks helped to keep terrorism high on the political agenda and maintained it as the principle security mission, which guided and shaped the others[47].

Over the last five years, however, security priorities have shifted at EU level. Counter-terrorism still remains a major area of action as recalled in the Internal Security Strategy adopted in 2010 and in the recent Communication of July 2010. However, the Internal Security Strategy and more importantly the Stockholm Programme of December 2009 also show that the EU's Security framework has broaden considerably with a stronger emphasis on citizens' direct interests, needs and perceptions. Thus the European security model has become an extremely wide and comprehensive concept taking into account risks and threats of any kind which could impact on citizens in a wider perspective and create a security problem in the broader sense. The Stockholm multi-annual strategic work programme and the action plan for 2010-2014 focus on measures in the area of Justice, Fundamental Rights and Citizenship (such as improvement of data protection in the EU) and in the Home Affairs area (such as strengthening cooperation in civil protection as well as disaster and border management). Consequently, the areas in which security relevant rules and regulations exist, are as numerous as diverse.

The EU security markets present additional specificities. They are highly regulated markets. The demand side is public and decentralised (national, regional, local), but also private. At the same time, the latter's demand for security is often driven by rules and regulations set by public authorities. Public actors shape the security market as both customers and regulators, which makes the regulatory environment inevitably even more complex.

In addition, in the EU, European law and national law co-exist since security matters in general remain Member States' prerogatives. The legal landscape has been simplified by the Lisbon Treaty which brought to an end the pillar structure of the EU, which included the legal personality of the European Communities and intergovernmental pillars for the Common Foreign and Security Policy and Justice and Home Affairs. Now that the EU has legal personality itself, it can be a party to international agreements which before had to be signed by each individual Member State. However, despite this simplification, many policy areas related to security still require unanimity (included in the 'special legislative procedures') rather than the new double qualified majority voting system that also gives a joint legislative role to the European Parliament (the 'ordinary legislative procedure' that used to be called co-decision).

---

44 Council of the European Union, *A Secure Europe in a Better World. European Security Strategy*, Brussels, 2003. Available at: http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

45 "Towards a European Security model", 23 Feb 2010, EU Council.

46 "The EU Counter-Terrorism Policy: main achievements and future challenges", Communication from the Commission, COM (2010) 386 final, 20.7.2010.

47 An Action Plan to Combat Terrorism was adopted in 2001, complemented in December 2005 by a Counter-terrorism Strategy which still guides EU institutions and Member States in their action to fight terrorism. The EU Security Strategy of 2003 guides the EU's Security and Defence Policy but was also strongly influenced by the terrorist attacks.

5.3 Main features of the EU regulations applying to the security sector

The main features of the regulatory environment for the security market in the EU are complexity and fragmentation. There is nothing like a single regulatory framework for the security market, but a multitude of different rules and regulations with different purposes for different areas.

The most relevant for industry are listed in Table 5.1 below. From this list of regulations we can draw some general conclusions on the main features of the EU legislation in the security area:

- Legislation at EU level is quite recent. It is mainly “threat” driven and follows specific events rather than a long term risk assessment and planning. It is also limited in scale and scope, with only a few binding legislative acts of interest for the supply side;
- EU legal instruments contain rather generic provisions and generally set minimum common requirements;
- The way and degree to which these EU legislative acts impacts on national law differ depending on the instrument used:
  - Directives harmonise and coordinate national legislation; i.e. Member States must transpose them into their national law and have some flexibility when they do so;
  - Regulations, by contrast, become directly part of national law and thus leave no room for interpretation;
  - At the same time, there are different types of implementing acts, which do not set new law but modify/update/revise existing EU-law;
  - All this contributes to a complex and sometimes confusing regulatory environment which reflects the division of competences between the EU and its Member States and still leaves room for national differences and thus fragmentation of the market;
  - From a security point of view and from an economic perspective, there is no common market in this area, which would require that operators implement security to similar requirements levels across countries;
  - There are also gaps in the EU legislative environment, such as the lack of common legislation in the field of ICT systems in Critical Infrastructures for instance.

Table 5.1 EU-level Security Regulatory Snapshot - Overview

Security sector	List and type of legislation	Objective - content	Scope	Field of application
Aviation	Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security, repealing Regulation (EC) No 2320/2002. Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008, amended by Regulation (EU) No 297/2010 of 9 April 2010. Regulation (EU) No 185/2009 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security. Regulation (EU) 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures. Regulation (EU) No18/2010 of 8 January 2010 amending Regulation (EC) No 300/2008 as far as specifications for national quality control programmes. Regulation (EU) No 72/2010 of 26 January 2010 laying down procedures for conducting Commission inspections.	Sets out common rules to safeguard civil aviation against acts of unlawful interference.	Common basic standards Compliance monitoring system	Application based Airport s, aircraft security Air transportation of persons and goods (Passengers, baggage, cargo) Security equipment Security processes Security systems

Security sector	List and type of legislation	Objective - content	Scope	Field of application
Maritime	Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security. Directive 2005/65/EC of 26 October 2005 on enhancing port security. Regulation (EC) No 324/2008 of 9 April 2008 laying down revised procedures for conducting Commission inspections in the field of maritime security.	Community measures to enhance port security.	Common basic rules Compliance monitoring system	Application based Maritime security Port security Infrastructure and equipment
(Critical) infrastructure protection	Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.	Sets a European process for identifying and designating European critical infrastructures (ECIs), and sets out an approach for assessing the need to improve their protection.	Common assessment criteria and requirements	Application based Energy and transport Security process
Customs	Regulation (EC) No 648/2005 of 13 April 2005 amending Regulation (EEC) No 2913/92 establishing the Community Customs Code.	Sets measures to tighten security for goods crossing international borders.		Application based Trade Goods Security system
Borders	Regulation (EC) No 562/2006 of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code).	Sets out the rules on crossing external borders and on reintroducing checks at internal borders		Application based Persons Security system and process
	Regulation (EC) No 444/2009 of 28 May 2009 amending Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.	Sets standards for security features and biometrics in passports and travel documents issued by Member states.	Common standards	Application based Document security (Passports and travel documents)

Security sector	List and type of legislation	Objective - content	Scope	Field of application
				Security technology biometrics
Data protection	Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.	Applies to protection of individuals with regard to the processing of personal data and on the free movement of such data.		Transversal Data process
Export controls	Regulation (EC) No 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology.	Sets a regime for controlling the export, transfer, brokering and transit of dual-use items.	General export authorisation « Compliance »	Transversal Dual-use products, equipment
Procurement rules	Directive 2009/81/EC of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC. Directive 2009/43/EC of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community ("Transfer Directive").	The Directive aims to apply internal market rules to products for defence and security. The Directive aims to harmonise the rules for the intra-Community transfer of defence-*related* goods[48]	Harmonisation	Transversal

[48] Though it always states for "military purpose" only, it might e.g. be of relevance if security forces acquire military equipment to carry out civ mil missions.

5.4 Assessment of the EU regulations applying to the security sector

In the following, we will assess in greater detail the regulatory framework of the various security segments.

5.4.1 Civil aviation security

See Table 5.2 for an overview of main regulations.

State of play

Security has been a matter of concern for civil aviation for several decades. However, in spite of its economic importance and cross-border dimension, aviation security was, up until 2002, been addressed on essentially a national level.

Following the terrorist attacks of 9/11, the Commission made a legislative proposal to bring aviation security under the EU's regulatory umbrella. The objective of the EU regulatory measures is to prevent acts of unlawful interference against air transportation. Therefore the first common regulations adopted in 2002[49] provided the basis for harmonisation of aviation security rules across the EU with binding effect. They closely followed international standards on aviation security as laid down in the Chicago Convention[50] and further developed through the International Civil Aviation Organisation (ICAO). In relatively short time the need for a more detailed harmonisation of the European rules became necessary and several acts of implementing legislation were added.[51] That regulatory framework has been fully completed and replaced by a new framework, in full effect from 29 April 2010, as laid down by Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security.

The main principle of European as well as international rules is to keep threat items such as arms and (liquid) explosives ("the prohibited articles") away from aircraft. For that reason every passenger, every piece of luggage and cargo departing from an EU airport, or coming from a third country and transferring through an EU airport, must be screened or otherwise controlled in order to ensure that no prohibited articles are being brought into security restricted areas of airports and/or on board aircraft. This common regulatory framework enables 'one-stop security' within the European Union which is the most important element of facilitation, both for industry as well as passengers. This implies that passengers (or luggage or cargo) arriving from another EU airport, do not need to be re-screened when transferring. Regulation (EC) No 300/2008 allows the concept of 'one stop security' to be extended, under certain conditions, to countries outside the EU.

The EU regulation (300/2008) lays down measures for the implementation and technical adaptation of common basic standards regarding aviation security to be incorporated into national civil aviation security programmes. In fact, each Member State is responsible for the adoption of a national civil aviation security programme which ensures the application of the common standards. The Regulation provides standards for *inter alia*, airport planning requirements, aircraft security, staff training and most importantly screening. Detailed rules on how these standards shall be implemented are defined in implementing acts, which include a list of screening and controlling

---

[49] Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (OJ L 355, 30.12.2002.

[50] Convention on the International Civil Aviation signed on 7.12.1944.

[51] The most important implementation acts are Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security (OJ L 89, 5.4.2003) replaced by Regulation (EC) No 820/2008, laying down measures for the implementation of the common basic standards on aviation security of 8.8.2008 (OJ L 221, 19.8.2008).

methods and technologies for passengers, baggage, cargo and courier from which the entities responsible for the implementation can choose the necessary elements in order to perform effectively and efficiently their aviation security tasks (search by hand, walk through metal detection equipment, conventional x-ray equipment, High definition x-ray, bio-sensory (sniffers, trace detectors, explosive detection dogs). The regulation also provides a set of specifications for aviation security equipment. For instance it defines requirements (security, operation requirements) for metal detection equipment.[52] It also provides standards and testing procedures for X-ray equipment (performance requirements[53] and operational requirements).

An important additional principle of the EU aviation security legislation is the possibility for Member States to set more stringent security measures in order to address a specific national security threat. Member States that take more stringent measures shall act on the basis of a risk assessment and in compliance with Community law. In addition, the measures shall be relevant, objective, non-discriminatory and proportional to the risk that is being addressed.

Comments

Many stakeholders consider that the principles set by the Regulations are not fully appropriate to address the challenges and threats faced by the aviation sector and to support industry develop innovative technology and solutions needed to face the new types of threats. The EU legislation is considered to have the following negative impacts on the market:

- **Burden:** Every change in law tends to add additional layers of measures. The result is that security checkpoints become overburdened with new equipment and the operation of newly developed security tasks;
- **Costs:** European airlines and airports in particular are concerned with the high costs incurred by the security measures they have to comply with[54]. In addition, public authority funding varies widely across the EU MS leading to distortions in competition between airports and air carriers in different countries. Often the business functionality remains the primary driver while security is considered a possible constraint at best;
- **Fragmentation:** MS' implementation of the EU Regulations has not been fully achieved. There are different national regulations for this market comprising for instance different national security levels and different testing procedures. This is further compounded by a lack of coordination between regulators and security solution providers;
- **Requirements:** existing security procedures are considered as a major cause of delays within an airport (limited throughput of current equipment, screening to all passengers). This situation could be improved via an EU harmonisation of procedures and of security capability requirements across countries. Indeed stronger coordination is required to ensure equipment interoperability and to avoid the proliferation of different systems at regional, national and EU level of the many new technologies and regulatory practices that will be developed in the next few years to address air transport security challenges;
- **Liability:** there is no European liability limitation framework for deployed security solutions in the EU. Without this manufacturers find it difficult to sell fully automated systems within the EU. An EU liability limitation framework would encourage innovation, efficiency and EU competitiveness in a cost efficient manner;

---

52 Equipment shall be capable of detection small items of different metals, with a higher sensitivity for ferrous metals in all foreseeable conditions.

53 Equipment shall provide for the necessary detection, measured in terms of resolution, penetration and discrimination, to ensure that prohibited articles are not carried on board aircraft.

54 For European airports, security alone represents up to 35% of their operating cost instead of 5% to 8% prior to the events of September 11. In 2002, 18 States and airports incurred an estimated expenditure of 2bn E on security related activities, according to the "Study on Civil Aviation Security Financing" (September 2004). EOS White Paper on Civil Aviation Security, October 2009.

- **Standards and Testing:** since 2001, operators have considerably improved passenger safety and security but they are still required to look for new technology developments to meet today's changing risk and threat environment (Improved detection technology capabilities providing for higher security of identity and luggage control such as standoff screening of passengers, detection/identification of dangerous liquids, etc.). However, there is no efficient and transparent test and validation procedure at EU level to follow today's advanced technology developments. The economic advantage of advanced baggage screening capability could be secured more cost efficiently with a common EU level technology testing system with common criteria for validation of air transport security solutions, ideally linked to common capability requirements across the EU. In addition, common standards on how to commission, execute and report test findings would be necessary, with the use for instance of an EU clearing house for test/qualification. Harmonisation of security technology standards with common criteria for the validation of air transport security solutions and services across all MS represent a big gap of the EU legislative framework.

The debate on Security (body) scanners is a good illustration of the various points mentioned above[55]. The current legislation does not permit airports to replace systematically any of the recognised screening methods and technologies by Security Scanners. Only a decision of the Commission supported by Member States and the European Parliament can be the basis for allowing Security Scanners as a further eligible method for aviation security. However, Member States are entitled to introduce Security Scanners for airport trials for a limited period of time [56] or as a more stringent security measure than those provided for by EU legislation.[57]. This results in different rules being used across the EU since Security Scanners are not systematically and uniformly deployed by Member States at their airports. In addition, their use is not harmonised in terms of operational conditions as they are regulated at national level.

To end the current fragmented situation wherein Member States and airports decide on an ad-hoc basis if and how to deploy Security Scanners at airports, the use of Security Scanners must be based on common standards, requesting basic detection performance and imposing safeguards to comply with European fundamental rights and health provisions. The Commission adopted mid-June 2010 a new Communication (COM (2010) 311 final) which provides a basis for discussing the key issues associated to the possible introduction of Security Scanners for screening persons at EU airports. It proposes a draft regulation with basic screening requirements for Security Scanners.[58] In addition, Common EU Standards for Security Scanners (technical standards and operational conditions) laid down in EU legislation are suggested in order to ensure a common level of protection of fundamental rights and health for European citizens. The Commission is currently assessing the next steps to take, including whether or not to propose an EU legal framework on the use of Security Scanners at EU airports.[59] On 24 May 2011 the European Parliament's Transport

---

55 Security Scanners is a generic term used for a technology that is capable of detecting metallic and non-metallic objects including plastics and liquid explosives carried under clothes. They could for instance replace walk-through metal detectors as means of screening passengers that today require screeners to undertake full body hand searches in order to achieve comparable results. They are also expected to assist in keeping throughput times at screening points at an acceptable speed.

56 Commission Regulation (EC) No 185/2010: Finland, France, The Netherlands, Italy and the UK have already introduced Security Scanners according to existing EU legislation.

57 See Article 6 on more stringent measures of Regulation (EC) No 300/2008.

58 Various technologies of Security Scanners are being developed. Existing and commercially available scanners generally use one of 4 technologies: Passive millimetre-wave; Active millimetre-wave; X-ray backscatter; X-ray transmission imaging. In particular, X-ray backscatter is the main technology deployed and operated in the US and the UK. There are several emerging technologies that have not yet obtained market maturity.

59 It is difficult to undertake a cost assessment of the deployment of Security Scanners. The Security Scanner market is an emerging market and only few individual purchases have been undertaken under purely commercial considerations. General information related to basic investment cost for equipment and use related costs are not yet available because existing European legislation does not allow for widespread deployment of this technology. Moreover, the choice airports

Committee approved a report that supports the use of scanners, subject to certain reservations. This signals the Committee's support for the use of scanners as an authorised method, ahead of a legislative proposal by the Commission which has to be adopted by the Parliament and Council by the ordinary legislative procedure.

5.4.2 Maritime and port security

See Table 5.3 for an overview of main regulations.

State of play

There are two main regulations of interest for the scope of our study. Taken together, the Directive on port security and the Regulation on ship and port facility security provide the necessary framework for protecting the whole chain of maritime transport logistics (from the ship to the port via the ship/port interface and the whole port area) against the risk of attacks on Community territory.

The main objective of the EU Regulation on ships and port facilities is to implement Community measures aimed at enhancing their security in the face of threats of intentional unlawful acts. The Regulation is intended to provide a basis for the harmonised interpretation, implementation and Community monitoring of the special measures to enhance maritime security adopted by the Diplomatic Conference of the International Maritime Organisation (IMO) in 2002, which amended the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and established the International Ship and Port Facility Security Code (ISPS Code). The amendments to the SOLAS Convention and Part A of the ISPS Code are mandatory, but subject to interpretation. Part B of the Code consists of recommendations which the Member States are called on to implement. The Regulation contains preventive measures and transposes the part of the SOLAS Convention on special measures to enhance maritime security and, at the same time, the ISPS Code, two of the cornerstones of maritime security at world level.

The Member States are required to communicate to the IMO, the Commission and the other Member States the information requested and the special measures adopted to enhance maritime security under the SOLAS Convention. Alongside this, each Member State must draw up a list of port facilities concerned on the basis of the port facility security assessments carried out and establish the scope of the measures taken to enhance maritime security.

The competent maritime security authority of that Member State should require each ship intending to enter port to provide, in advance, information concerning its international ship security certificate and the levels of safety at which it operates and has previously operated. Member States are required to apply the new security measures to international shipping to Class A passenger ships operating domestic services.

The Commission carries out security inspections at port facilities and companies in the Member States. These inspections are prepared with assistance from the European Maritime Safety Agency and are conducted by inspectors from the Member States.

---

have to assemble security methods will make overall costs closely dependant on the security options individual airports will design and apply. According to information received from manufacturers and based on procurements recently done inside and outside the EU, the purchase cost of a basic Security Scanner per equipment ranges between EUR 100 000 and 200 000 (not including possible upgrades, maintenance or other after-sales services). Expected costs are supposed to decrease in the future due to higher production numbers. Depreciation for aviation security equipment is commonly done over a period of 5 to 10 years.

The Directive on port security complements the measures to enhance the security of ships and port infrastructure. Ports are often the focal point for shipments of dangerous cargo, for major chemical and petrochemical production centres, and/or situated near cities. It is clear that terrorist attacks in ports can easily result in serious disruptions to transport systems and the neighbouring population.

The main objective of the Directive is to introduce a security system in all port areas guaranteeing a high and comparable level of security in all European ports. The Directive applies to people, infrastructure and equipment (including means of transport) in ports and adjacent areas.

Member States must designate a port security authority for each port. One must be designated for several ports. This authority is responsible for identifying and taking the necessary port security measures in line with port security assessments and plans. Member States must also ensure that port security plans are developed, maintained and updated, with a detailed description of the measures taken to enhance port security (such as the conditions of access to ports or the measures applicable to baggage and cargo). Member States must monitor security plans and their implementation, and specify penalties for non-conformity.

Different security levels are established in line with the perceived risk (normal, heightened or imminent threat), namely:

- **Security level 1:** the level for which minimum protective security measures must be maintained at all times;
- **Security level 2:** the level for which appropriate additional protective security measures must be maintained for a period of time as a result of heightened risk of security incident;
- **Security level 3:** the level for which further specific protective security measures must be maintained for a limited period of time when a security incident is probable, although it may not be possible to identify the specific target.

Member States must communicate the security level in force for each port as well as any changes thereto. The Member States accredit a security officer in each port, who may be common to them all. These officers act as the contact point for port security related issues and should have sufficient authority and local knowledge to adequately ensure and coordinate the establishment, updating and follow-up of port security assessments and port security plans.

Member States must ensure that port security assessments and port security plans are reviewed every time security-relevant changes occur, and at least every five years.

Comments

The ISPS code, agreed by the IMO and implemented by the EU's Regulation on ships and port facilities, provides the framework for common standards in maritime security. A certain level of certification exists, such as the International Ship Security Certificate (ISSC) that requires the good maintenance of records and retrieval of security records and contacts between the ship and port facilities. Under the rules of the Regulation, ships entering port are required to provide this certificate in advance to the national authorities.

There are currently a large number of new technologies being developed for maritime surveillance, specifically vessel tracking, including Advanced Information Systems (AIS) and Long Range Information Tracking. While they have different uses, their ability to control illegal use of shipping is among the most important. However, as they are at an early stage and current legislation does not require their use, then the conditions for certification may not yet be present.

5.4.3 *Critical infrastructure protection (CIP)*

See Table 5.4 for an overview of main regulations.

State of play

Critical infrastructure can be damaged, destroyed or disrupted by natural disasters, negligence, accidents, criminal activity, and malicious behaviour and also by deliberate acts of terrorism[60]. The failure of part of the infrastructure (even in different European countries) could lead to failures in other sectors, causing a cascade effect because of the synergistic effect of infrastructure industries on each other. Therefore, the damage or loss of a piece of infrastructure in one Member State may have negative effects on several others and on the European economy as a whole.

The terrorist attacks in Madrid and London highlighted the risk of terrorist attacks against European infrastructure and were the main drivers for action in this field. The EU responded in 2004 with the adoption of a European Programme for Critical Infrastructure Protection (EPCIP) to provide a common level of protection in Europe and coordinate MS's efforts in this field. The objective was to make sure that each MS would provide adequate and equal levels of protection concerning their critical infrastructure and that the rules of competition within the internal market would not be distorted. Critical infrastructure protection is by nature a very complex and far reaching issue and EPCIP opened a new policy area within the EU cutting across a large number of critical infrastructure sectors and organisational boundaries.

More specifically, the Commission adopted in October 2004 a Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism"[61] which provided a very broad definition of critical infrastructures: " those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States." They can cover therefore a wide range of sectors: energy installations and networks, communications and information technology; finance (banking, securities and investment); health care; food; water (dams, storage, treatment and networks); transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems); production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials); government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

In 2006, the Commission adopted a Directive focusing on the identification and designation of critical infrastructure of a European dimension (European Critical Infrastructure or "ECI"): "Critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States". The Directive also provides a European procedure for the identification of ECI, in particular the obligation for Member States to inform those that may be affected, but also the establishment of Operator Security Plans (OSPs) for the identification and designation of ECI. This was complemented in 2008 by a Council Directive (2008/114/EC) on the identification and designation of ECI and the assessment to improve their protection in the field of energy and transport. Within the Directive a distinction is made between critical infrastructure and European critical infrastructure:

---

[60] The consequences of attacks on the control systems of critical infrastructure may vary. It is commonly assumed that a successful cyber-attack would cause few, if any, casualties but might result in the loss of vital infrastructure service. An attack on the control systems of a chemical or liquid gas facility might lead to more widespread loss of life as well as significant physical damage.

[61] Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism [COM (2004)702 final - Not published in the Official Journal].

- "'[C]ritical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;
- 'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure".

Comments

The main feature effect of this legislation is that MS and the owners/operators are the ultimate responsible for protecting ECI despite the introduction of a European procedure for the identification and designation of ECI. This leads to a series of difficulty, gaps and challenges.

By mandate the Commission is limiting its activity to "European" Critical Infrastructures, i.e. those having a trans-border dimension. However, MS economies, citizens and governments are mainly relying on local and national infrastructures. From a market perspective, if we had an effective European approach facilitating the protection of infrastructures throughout Europe by implementing common solutions and services in the different EU countries, costs for development would be reduced and duplication of technologies avoided.

The concept of OSPs for instance, as defined by the European Critical Infrastructure Directive and initially applied for Energy and Transport infrastructures is an example of a practical progress already made towards collective resilience building. However being a Directive, it needs to be transposed into national law, which leaves Member States some room for manoeuvre. Consequently, implementation differs between countries, creating potential security imbalances between MS, a patchwork of "good and bad security"[62] with varying degrees of verification across MS. There are no EU guidelines across countries for common terms, approaches, methods and common requirements on how these plans should be applied resulting in a lack of comprehensive concerted action and interoperability.

The EU has also adopted in some areas legislative measures setting minimum standards for infrastructure protection. This is notably the case in aviation and maritime transport (see above). However this minimum standard approach also results in barriers to trade and fragmentation of markets as has been shown in the precedent sections.

In other CI areas EU legislation is lacking, which impedes the development of a common approach between MS to address security threats efficiently. This is the case notably for ICT. ICT systems have become key components of many Critical Infrastructures and in some cases constitute themselves a CI. As such their disruption, malfunction or compromise can seriously impact our societal and individual wellbeing. Even though the Communication from the Commission on Critical Information Infrastructure Protection (COM(2009)149 final, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience") constitutes a major step forward in the protection against large scale attacks and disruptions, there is still no EU legislation in this area. The EU market for ICT/ cyber security is wide and unstructured. The protection of these essential assets remains insufficient and often also fragmented at national level. ICT security is still perceived as a constraint rather as a compulsory feature or as an opportunity by operators who overlook the return on investment of secure operations versus the high costs

[62] EOS White Paper on Energy Infrastructure Protection and Resilience, November 2009.

incurred through intentional or accidental security breaches. No incentive is provided to CI operators and IT suppliers to ensure that it is built-in from the start and managed during operations. Industry for instance supports a Secure-by-Design framework (security designed into the systems from the beginning) but if security is not expressed as a requirement by a customer, it is unlikely that suppliers will include it in their proposed solutions since the extra cost will make them uncompetitive to less secure options.

5.4.4 Border security

See Table 5.5 for an overview of main regulations.

State of play

Passenger flows at the external borders of the EU have been growing and will continue to increase. Border control poses therefore an ever important challenge. It consists of the verification of people, vehicle and goods at regulated land or maritime check points and involves identity checks and information searches against various databases of persons to be either apprehended or denied entry to the territory and the use of advanced techniques for identifying the risk.

Border Control covers two types of activities: Border Surveillance and Border Checks. The Schengen Convention and the Schengen Borders Code define three types of external borders: air borders (airports), sea borders and land borders (rail and road). Checks can be:

- "pre-border" (with the objective of transmitting information on passengers before their arrival at the Border Check Point. The information transmitted is based on Advanced Passenger Information (API) and Passenger Name Record (PNR), the latest restricted to borders;
- "first-line": checks on the entry and exit of any traveller crossing the Schengen area to verify the validity of the Visa;
- "second-line": takes place when an officer identifies an abnormality during the first line check and further thorough checks are needed.

There are currently three large scale information technology (IT) systems in this area: SIS II, VISA and EURODAC. The Schengen Information System (SIS) is a computer network for the collection and exchange of information relating to immigration, policing and criminal law for the purpose of law enforcement and immigration control. The system has been storing a series of data but due to technology obsolescence, a second generation (SIS II) which will include new types of data and new functionalities such as the possibility to include biometric data, was established in 2006. This system facilitates the exchange of information on person and objects between national authorities responsible for border control. The Visa Information System (VIS) established in 2008 is a system for the exchange of visa data in order to implement the visa policy, contribute to the fight against internal terrorism and fight against illegal immigration. EURODAC a Union-wide IT system, was created as a mechanism for determining responsibility for asylum application lodged in one of the EU MS. On June 2009, the Commission adopted a legislative proposal package to establish a new Regulatory Agency that would be responsible for the operational management of those systems and of other large-scale IT systems in this area. The Agency will be established in 2011 and presumed to become operational in 2012. Therefore, the Agency will cover matters related to checks on persons at external borders as well as measures in the area of illegal immigration and residence. It also supports the procedures for issuing visas by MS and the determination of which MS is responsible for considering an application for asylum.

In addition to that the EU adopted Regulation to provide enhanced protection for passports and travel documents against falsification. In the aftermath of the 11 September 2001, the Commission was asked by MS to take immediate action to improve document security. It was therefore decided

to integrate biometrics in European passports with identifiers consisting of a facial image and fingerprints, making it possible to combat fraud and falsification more effectively. The introduction of biometrics in passports and travel documents also reflects the need for Member States participating in the United States Visa Waiver Program to align themselves with the relevant US legislation, so that their nationals may enter US territory without a visa. Therefore, under this regulation, biometric identifiers were perceived as a mean to harmonising national legislation.

Common measures were taken on biometric identifiers and data for documents for third-country nationals, EU citizens' passports and information systems. Passports and travel documents will include a high-security storage medium for memorising computerised data that will have sufficient capacity to guarantee the integrity, authenticity and confidentiality of that data. The storage medium will contain a facial image and two fingerprints taken flat. These data, which will be in interoperable formats, will be secured. Passports and travel documents will have to be issued as individual documents in accordance with international requirements.

In accordance with international standards, the Commission established additional technical specifications, such as:

- additional security features, notably with a view to combating counterfeiting and falsification;
- the storage medium and its security;
- common quality requirements for the facial image and the fingerprints.

The biometric features in passports and travel documents will be used only for verifying the authenticity of the document and the identity of the holder, who will have the right to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure. The collection and storage of biometric data will be exclusively for the purpose of issuing passports and travel documents.

Each Member State will designate one body for printing passports and travel documents. Under the provisions of the Schengen *acquis*, Denmark, the United Kingdom and Ireland do not take part in this regulation and so are not bound by it.

Comments

The legal framework in the area of Border Control is characterized by variable geometry. Ireland and the UK participate in EURODAC but are only partly involved in SIS II, and do not participate in VISD, while Denmark is involved in all three systems on a different legal basis. The legal framework is also complex. Due to the former cross-pillar elements of the SIS II, the legal framework of SIS II is composed of 'first pillar' Regulations and Decisions and 'third pillar Decisions'. Although this distinction disappeared upon entry of the Lisbon Treaty, existing instruments still reflect the former pillar structure. As opposed to the SIS II, VIS was established under the former first pillar. However a VIS third pillar instrument was adopted to allow designated law enforcement authorities to access the system for consultation regarding the commitment of certain offenses. EURODAC was established under the former first pillar.

5.4.5 Custom controls

See Table 5.6 for an overview of main regulations.

State of play

The establishment of a Customs Union was an important step in the process European integration. In 1992 the Community Customs Code was adopted to codify and simplify Community customs law and replaces many different pieces of fragmented legislation. Regulation 2913/92 has been in force

since 1st January 1994 and includes provisions on import and export duties, introduction of goods into the customs area and their subsequent treatment or use. The code is implemented via Regulation 2454/93 which was adopted shortly after to standardise and simplify the existing implantation provisions. Procedures covered by the implementing rules include providing customs authorities with information on classification and origin of goods, the application of the Community customs tariff (based on valuation of goods according to WTO agreements), responsibilities and powers of customs officials with regard to controlling imports, customs declarations, approval of treatment or use and so called 'privileged operations' (goods originating from the customs area which are re-exported).

Since the Community Customs Code was established there have been several revisions to the regulations. Minor changes in 1997 and 1999 were followed by more substantial amendments in 2000 that aimed to make simplifying rules and procedures, preventing fraud, facilitating the use of new technologies and in general making procedures more efficient.

In 2005 amendments were made to tighten security for the movement of goods across international borders. This followed a growing concern about security threats in international trade, reflecting in the Commission Communication on the role of customs in the integrated management of external borders[63]. The communication argued that the controls in place were not adequate to protect Member State against threats from terrorism and criminality, health and safety risks to consumers, and environmental risks. One of the main weaknesses was the lack of harmonisation of controls among Member States based on varying procedures, equipment and resource allocation. The 2005 amendments aimed to tackle these challenges by requiring economic operators to provide customs authorities with details of goods before they are imported into the EU or exported from it, through 'one stop shops'. In addition, common methods for risk-assessment analysis were introduced based on computerised systems.

In 2008 a modernised customs code was agreed[64], to follow recent technological developments in the field of customs control. However, the new code can only be implemented once the implementing rules become applicable and it has taken a long time to develop computer systems in line with the rules. The main changes foreseen in the new code are:

- Rationalisation of the legal framework and the definition of custom rules and procedures (including fewer procedures);
- Greater standardisation of customs rules and their implementation through IT systems to manage decisions, simplifications and guarantees related to the rights and obligations of economic operators;
- Simplification of customs procedures and the creation of a centralised customs clearance system (EU level management);
- IT system for declaration and data exchange; and
- Interoperability of national customs systems.

Comments

The legislative framework for customs control reflects the need for simplified procedures that are based on new technologies while at the same time ensuring a high level of security from increasing threats linked to goods entering the European Union. The 2005 amendments were made urgently because of the growing security threats from terrorist activities (notably after the 9/11 attacks on the United States). Both developments in the legislative framework imply a growing demand for equipment and technology that efficiently and securely controls the EU's external borders.

---

63 COM(2003) 452 final - Official Journal C 96 of 21.4.2004.

64 The new code was introduced via Council Regulation 450/2008.

5.4.6 *Export controls*

See Table 5.7 for an overview of main regulations.

State of play

The Directive 2009/81/EC on the procurement of defence and sensitive security supplies, works and services entered into force on 2009. The Directive 2009/81/EC aims primarily at bringing the bulk of defence procurement into the Internal Market, thereby opening up national markets to EU-wide competition and establishing the basis for a European Defence Equipment Market. However the procurement rules laid down in the Directive also applies to security markets. This Directive is thus the only piece of EU legislation which covers the whole spectrum of military and non-military security, including even contracts awarded by private operators of critical infrastructures in the water, energy and transport sectors.

In the field of defence, its scope is (at least indirectly) defined by military lists. In the field of security, by contrast, its scope is defined in a very generic way: The Directive applies to "sensitive procurements" and defines the latter as "*equipment, works and services for security purposes, involving, requiring and/or containing classified information.*" This very generic approach makes it possible to apply the Directive across the entire spectrum of security areas. In this context, recital 11 specifies that *"in the specific field of non-military security, this Directive should apply to procurements which have features similar to those of defence procurements and are equally sensitive. This can be the case in particular in areas where military and non-military forces cooperate to fulfil the same missions and/or where the purpose of the procurement is to protect the security of the Union and/or the Member States, on their own territory or beyond it, against serious threats from non-military and/or non-governmental actors. This may involve, for example, border protection, police activities and crisis management missions".*

Comments

MS are still in the process of transposing this Directive into their national legislation. To which degree the Directive will open national security markets to EU-wide competition in the security market is hard to predict for various reasons. There are hardly any figures on the size of these markets, let alone their openness. There is therefore no reliable baseline for an impact assessment[65].

In addition, up until now, Member States have exempted their sensitive security procurements via an exclusion clause of the General Public Procurement Directive 2004/18/EC, which states that this Directive "*shall not apply to public contracts when they are declared to be secret, when their performance must be accompanied by special security measures... or when the protection of the essential interests of that Member Sate so requires*" (Article 14). The question for the future is twofold:

- How many contracts which have been exempted up until now from Directive 2004/18/EC for reasons of sensitivity will in the future be awarded according to the rules of the new Directive 2009/81/EC; and
- What is the economical/financial value of these contracts (in particular in comparison to defence procurement, where production volumes and orders are normally much bigger than in security)?

The new Directive contains a number of provisions specifically adapted to the special features of security procurement. For security customers, security of classified information and reliability of suppliers are probably particularly important; the Directive allows making such requirements in

[65] See DefSec report, p. 183-186.

different forms (in particular as selection criteria and/or contract execution conditions). These safeguards are expected to limit the cases where contracting authorities "have" to derogate in order to protect their essential security interests to really exceptional cases.

At the same time, however, the Directive itself contains a number of exclusions which are particularly relevant for security. According to Article 13, the Directive shall not apply to "*contracts for which the application of the rules of this Directive would oblige a Member State to supply information the disclosure of which it considers contrary to the essential interests of its security*" (13a), nor to "*contracts for the purpose of intelligence activities*" (13b). The first exclusion is an almost literal repetition of Article 346 (1)(a) TFEU and therefore in principle redundant, since the Directives applies by definition only subject to Article 346 (1)(a). The second exclusion is at the same time limited (intelligence) and generic (activities). In this context, recital 27 specifies that *"some contracts are so sensitive that it would be inappropriate to apply this Directive, despite its specificity. That is the case for procurements provided by intelligence services, or procurements for all types of intelligence activities, including counter-intelligence activities, as defined by Member States. It is also the case for other particularly sensitive purchases which require an extremely high level of confidentiality, such as, for example, certain purchases intended for border protection or combating terrorism or organised crime, purchases related to encryption or purchases intended specifically for covert activities or other equally sensitive activities carried out by police and security forces.* This list of cases potentially covered by the exclusion, indicates that Article 13 (a) and (b) are apparently tailor-made to security (rather than defence) concerns. The Directive thus takes into account that non-military security procurements can often be even more sensitive than military procurements and accepts that in these cases transparent procurement procedures and trans-national competition may not be appropriate.

In principle, the existence of common procurement rules in the security area should lead to greater market openness for European companies. However, numerous exceptions and the margin of manoeuvre MS will still have in the definition of their security interests and requirements make it doubtful that the market will become considerably more transparent and open. The situation may be different for private operators of critical infrastructures who already face competition in their own markets and may therefore be ready anyway to choose the economically most advantageous security solution, no matter whether it comes from a national or non-national supplier .In addition, the limits of the security regulatory framework highlighted in the previous section (absence of common requirements, different national standards and procedures) also represent obstacles to the opening-up of the security market.

It will be interesting to see whether the Defence Directive will help break the existing national defence procurement markets and create a single EU market for the procurement of defence equipment. Many share the view that the success of the new measures will mostly depend on the European Commission and bidding companies' readiness to intervene and challenge Member States' routine use of the Article 346 (previously Article 296 EC) exemption.

In line with the European Court rulings, a Member State would now have the burden to prove that the use of the new defence procurement procedures would not be sufficient, in the specific case, to protect its essential security interests. The new Directive provides a clear legal basis to bidders who are excluded from a contract award procedure that is limited to domestic suppliers, on the ground of protection of national security interests, to complain before the European Commission. Bidders who have not previously considered this option, may wish to follow closely the development of this market, and the procedures available at both the EU and national level to challenge procurement decisions.

5.4.7 *Data protection*

See Table 5.8 for an overview of main regulations.

State of play

Data protection in the EU is based on important developments in jurisprudence relating to privacy and human rights law. Article 8 of the Charter of Fundamental Rights recognises the right to the protection of personal data, which must be processed with the consent of the individual concerned for specific purposes. Privacy is also enshrined in the European Convention on Human Rights, which insists on the right to a person's "*private and family life, his home and his correspondence*", except for well-defined circumstances such as national security. Furthermore, these rights have been enforced through various rulings by the European Court of Justice.

The lack of harmonisation in data protection rules restricts the movement of data and this problem had been identified by the OECD in the early 1980s, which formulated a set of guidelines for "the Protection of Privacy and Trans-Border Flows of Personal Data"[66]. The introduction of varying national legislation threatened to interrupt the flow of data which was becoming particularly important for many services sectors such as banking and insurance.

In the EU, rules on data protection are based on the Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has two main objectives: to remove barriers to the free movement of data between Member States while protecting the right of privacy of individuals. The Directive applies to both data processed by automated means (e.g. computer databases) and non-automated means (e.g. traditional filing systems). The two main exceptions to the Directive are for processing of data related to everyday personal and household activities and for those activities that fall outside the scope of Community law such as defence and security.

The Data Protection Directive in fact follows closely the OECD guidelines referred to above, in particular the principles on the processing of data.

- Firstly, data should be processed according to the law and only for clearly defined purposes. It must have a legitimate use; in other words data can only be processed with the consent of the individual (or 'data subject') and for specified reasons including contractual obligations, legitimate commercial interests and public services;
- Secondly there are limits to the type of data processed, which excludes personal data such as ethnicity or religious/political beliefs;
- Thirdly, data should be accessible to the data subject as well as information on how it is being processed; any data which does not comply with the rules of the Directive should be deleted. Furthermore, the data subject has a right to object to data being processed for legitimate reasons;
- Fourthly, data must be processed securely and confidentially after the notification of the national supervisory authority;
- Finally, there are a number of exemptions from the Directive, notably in relation to national security and defence, or the prosecution of criminal offences.

According to the provisions of the Directive, the Member States have established independent authorities which are responsible for the application of the rules in their respective territories.

---

[66] See OECD's website for more information: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

In 2003 the Commission published a report on the implementation of the Directive[67]. It found that the basic objectives of removing the barriers to free movement of data while ensuring a high level of data protection had been met. However, it also reported that divergences in the transposed legislation across the EU prevented multinational organisations from developing pan-European policies on data protection. Accordingly, a 'road map' was established to ensure greater legislative harmonisation. Four years later, a Communication from the Commission[68] on the roadmap reported improved implementation. The differences in national legislation did not cause too much of an administrative or financial burden. However, there remained several legal obstacles to the protection and legitimate use of private data for the purposes of public security, since these lay outside the scope of the directive[69]. These legal obstacles have been resolved through additional Community legislation, namely:

- In the framework of police and judicial cooperation, a Council Framework Decision[70] laid down the principles of lawfulness, proportionality and purpose in order to guarantee a high level of public safety while ensuring the protection of basic rights and freedoms with regards to privacy. Data can only be collected and processed for specified, explicit, and legitimate purposes and may only be used for the originally defined purposes (with few strict exemptions). Independent national bodies set up under the Data Protection Directive are responsible for the monitoring of the rules;
- The increased use of electronic communications had reduced the commercial necessity to retain data and yet this was considered vital for ensuring public security. Therefore a Directive[71] was adopted to ensure that data was retained by placing certain obligations on telecommunications and IT providers, while providing for financial compensation to cover the increased financial burden.

Despite the generally positive assessment of the Data Protection Directive's implementation, technological developments and globalisation have changed the context and requirements for regulation and thus the Commission launched a process to review the Directive in 2009. A Communication on Data Protection[72] was published by the Commission at the end of 2010 following a stakeholder consultation. New legislation will be put forward in 2011. The focus of the review is on the Directive's twin objectives; to ensure a high level of protection of personal data (privacy) while supporting the free flow of information (internal market).

The Communication calls for even better implementation of the Directive and closer harmonisation of national rules in order to give multi-national companies legal certainty when operating within the EU's internal market. Currently they have to adapt to several different sets of legislation which also increases the administrative and financial burden for them. Other concrete suggestions for reform are:

- Revision and simplification of the notification system (to the data operating companies) to reduce the administrative burden, with the possibility of an EU-wide registration form;

---

67 Report from the Commission: First Report on the implementation of the Data Protection Directive, COM(2003) 265 final.

68 Communication from the Commission to the Council and the European Parliament on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final.

69 This was confirmed by ECJ case law (Joined cases C-317/04 and C-318/04 of 30 May 2006).

70 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

71 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

72 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union COM(2010) 609 final.

- Clarify the responsibilities of Member States and on the regulation of data controllers in third countries;
- Enhancing the responsibility of data controllers through policies and mechanisms to comply with data protection rules (including the obligation to appoint an independent data protection officer and carry out data protection impact assessments);
- Self-regulatory initiatives, including the promotion of Codes of Conduct;
- EU certification schemes (e.g. 'privacy seals') for privacy compliant processes, technologies, products and services.

When making proposals for the revision of the Data Protection Directive, the Commission intends to include the provisions for the processing of data in the area of police and judicial cooperation in criminal matters. This is in light of the changes to EU primary law, specifically the abolishment of the pillar structure by the Lisbon Treaty[73] and a new comprehensive legal basis for the protection of personal data.

Comments

Multi-national companies operating in various Member States have occurred substantial costs due to the lack of harmonisation of the Directive's provisions. The revision of the Directive but also its better implementation across the EU will help to increase the free movement of data. In order to support the internal market objective, the Commission is exploring the creation of EU certification systems. This will be important not only for individuals whose data is used, but also for the responsibility of data controllers who will be able to prove that they have met the legal requirements by using certified technologies, products or services. The crucial factor of the success appears to be how credible certification systems are and if they meet international technical standards. Further steps to simplification of the regulatory environment, including the abolishment of the distinction between commercial uses and judicial/police cooperation also offer the potential for greater standardisation in the market related to privacy technologies.

[73] Officially called the Treaty on the Functioning of the European Union.

Table 5.2 Civil aviation security: EU regulatory framework

<table>
<tr><th colspan="2">Civil aviation security</th></tr>
<tr><td colspan="2">International legislation
Chicago Convention on International Civil Aviation, sets international standards on aviation security (Annex 17), further developed through the ICAO (International Civil Aviation Organization) civil aviation security programme and seeking to safeguard civil aviation and its facilities against acts of unlawful interference.</td></tr>
<tr><td>EU legislation</td><td>National responsibility</td></tr>
<tr><td>List of legislative acts:
Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008, amended by Regulation (EU) No 297/2010 of 9 April 2010.

Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security.

Regulation (EU) 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures.

Regulation (EU) No18/2010 of 8 January 2010 amending Regulation (EC) No 300/2008 as far as specifications for national quality control programmes.

Regulation (EU) No 72/2010 of 26 January 2010 laying down procedures for conducting Commission inspections in the field of aviation security to monitor the application by Member States of Regulation (EC) No 300/2008.

Objectives
The EU legislation provides the basis for a common interpretation of Annex 17 to the Chicago Convention on International Civil Aviation. In order to protect the air transportation of persons and goods, the EU has established common rules applicable across the EU to safeguard civil aviation against acts of unlawful interference.</td><td>MS are responsible for the implementation of the common basic standards. they must:
• designate a single appropriate authority responsible for the implementation of the common basic standards;
• define national civil aviation security programmes describing the measures required by operators and entities for implementing the basic standard (technical adaptation of common basic standards regarding aviation security to be incorporated into national civil aviation security programmes);
• define national quality control programme to monitor compliance with the EU regulation and with national civil aviation security programmes.

Operators and entity are responsible for implementing:
• airport security programmes setting out methods and procedures to be used by airport operators to ensure compliance with the EU regulation and with the Country’s national civil aviation security programme;
• air carrier security programmes setting out methods and procedures to be used by the air carrier to ensure compliance with the EU regulation and with the Country’s national civil aviation security programme;
• entity security programmes setting out methods and procedures to be used by the Entity to ensure compliance with the EU regulation and with the Country’s national civil aviation security programme.

Derogations
Member States may derogate from the common basic standards referred to Regulation (EC) No 300/2008 and adopt alternative security measures that provide an adequate level of protection on the basis of a local risk assessment at airports or demarcated areas of airports where traffic is limited to one or more of the</td></tr>
</table>

Civil aviation security	
Means/scope The means of achieving the objectives are the setting of: • common rules and common basic standards on aviation's security; • mechanisms for monitoring compliance. **Field of application:** The regulation's provisions apply to: • all airports; • parts of airports; • all operators, including air carriers; • all entities inside or outside airport premises providing services to airports located in an EU country that are not used exclusively for military purposes. **Provisions on common basic standards:** The regulation introduces common basic standards for protecting civil aviation covering: • airport security; • demarcated areas of airports; • aircraft security; • passengers and cabin baggage; • hold baggage; • cargo and mail; • air carrier mail and air carrier materials; • in-flight and airport supplies; • in-flight security measures; • staff recruitment and training; • security equipment. The regulation provides general measures with criteria and conditions for the common basic standards : a. methods of screening allowed; b. categories of articles that may be prohibited; c. as regards access control, grounds for granting access to airside and security restricted	following categories: 1. aircraft with a maximum take-off weight of less than 15 000 kilograms; 2. helicopters; 3. law enforcement flights; 4. fire suppression flights; 5. flights for medical services, emergency or rescue services; 6. research and development flights; 7. flights for aerial work; 8. humanitarian aid flights; 9. flights operated by air carriers, aircraft manufacturers or maintenance companies, transporting neither passengers and baggage, nor cargo and mail; 10. flights with aircraft with a maximum take-off weight of less than 45 500 kilograms for the carriage of own staff and non fare-paying passengers or goods as an aid to the conduct of company business. MS are allowed to apply more stringent measures than the common basic standards providing that those measures are relevant, objective, non-discriminatory and proportional to the risk being addressed. The Commission must be informed and communicates the information to the other EU countries. **Quality control** The EU Regulation sets common specifications for the national quality control programme to be implemented by each Member State in the field of civil aviation security (Aim = more harmonisation in 27 EU MS).

areas;

d. methods allowed for the examination of vehicles, aircraft security checks and aircraft security searches;
e. criteria for recognising the equivalence of security standards of third countries;
f. conditions under which cargo and mail shall be screened or subjected to other security controls, as well as the process for the approval or designation of regulated agents, known consignors and account consignors;
g. conditions under which air carrier mail and air carrier materials shall be screened or subjected to other security controls;
h. conditions under which in-flight supplies and airport supplies shall be screened or subjected to other security controls, as well as the process for the approval or designation of regulated suppliers and known suppliers;
i. criteria for defining critical parts of security restricted areas;
j. criteria for staff recruitment and methods of training;
k. conditions under which special security procedures or exemptions from security controls may be applied.

The regulation also lists detailed measures that provide the requirements and procedures for the implementation of the common basic standards :

a. requirements and procedures for screening;
b. a list of prohibited articles;
c. requirements and procedures for access control;
d. requirements and procedures for the examination of vehicles, aircraft security checks and aircraft security searches;
e. decisions to recognise the equivalence of security standards applied in a third country;
f. as regards cargo and mail, procedures for the approval or designation of, and the obligations to be fulfilled by, regulated agents, known consignors and account consignors;
g. requirements and procedures for security controls of air carrier mail and air carrier materials;
h. as regards in-flight supplies and airport supplies, procedures for the approval or designation of, and the obligations to be fulfilled by, regulated suppliers and known suppliers;
i. definition of critical parts of security restricted areas;

Civil aviation security	
j. staff recruitment and training requirements; k. special security procedures or exemptions from security controls; l. technical specifications and procedures for approval and use of security equipment; and m. requirements and procedures concerning potentially disruptive passengers. **Provision on compliance** The Commission conducts inspections to monitor the application of the common basic standards by EU countries.	

Table 5.3 Maritime and port security: EU regulatory framework

Maritime and port security	
International legislation: International Maritime Organisation (IMO) of 2002, which amended the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and established the International Ship and Port Facility Security Code (ISPS Code).	
EU legislation	**National responsibility**
List of legislative acts Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security. Directive 2005/65/EC of 26 October 2005 on enhancing port security, complementing Regulation (EC) No 725/2004. Regulation (EC) No 324/2008 of 9 April 2008 laying down revised procedures for conducting Commission inspections in the field of maritime security. **Objectives** The main objective of the EU legislation is to introduce Community measures to enhance port security in the face of threats of security incidents. The Regulation is intended to provide a basis for the harmonised interpretation and implementation and Community monitoring of the special measures to enhance maritime security adopted by the Diplomatic Conference of the International Maritime Organisation (IMO) in 2002. **Means, scope:** The measures consist of: 1. common basic rules on port security measures; 2. implementation mechanism for these rules; 3. compliance monitoring mechanisms. **Field of application** The Legislation applies to: • people; • Infrastructure; • equipment (including means of transport) in ports and adjacent areas. **Provisions on monitoring compliance** Procedures for conducting Commission inspections to monitor the application of EU Regulation at the level of each Member State and of individual port facilities and relevant companies.	**MS** are responsible for: • designating a port security authority for each port. This authority is responsible for identifying and taking the necessary port security measures in line with port security assessments (annex I) and plans (annex II); • ensuring that port security plans are developed, maintained and updated, with a detailed description of the measures taken to enhance port security (such as the conditions of access to ports or the measures applicable to baggage and cargo); • monitoring security plans and their implementation, and specify penalties for non-conformity; • accrediting a security officer in each port responsible for ensuring and coordinating the establishment, updating and follow-up of port security assessments and port security plans; • communicating the security level in force for each port as well as any changes. Different security levels are established in line with the perceived risk (normal, heightened or imminent threat), namely: - security level 1: minimum protective security measures must be maintained at all times; - security level 2: appropriate additional protective security measures must be maintained for a period of time as a result of heightened risk of security incident; - security level 3: specific protective security measures must be maintained for a limited period of time when a security incident is probable, although it may not be possible to identify the specific target.

Table 5.4 Critical infrastructure protection: EU regulatory framework

(Critical) infrastructure protection	
International legislation: not applicable	
EU legislation	**National responsibility**
List of legislative acts Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. **Objectives** The EU's objective is to provide a common level of protection in Europe and coordinate MS's efforts in this field. The objective is to make sure that each MS provide adequate and equal levels of protection concerning their critical infrastructure and that the rules of competition within the internal market are not distorted. **Means, scope:** The Directive establishes a European process for identifying and designating European critical infrastructures (ECIs), and sets out an approach for assessing the need to improve their protection. **Field of application** The Directive's scope concentrates on the energy and transport sectors and their subsectors: • Energy; • Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity security systems and procedures; • Oil: Oil production, refining, treatment, storage and transmission by pipelines; • Gas: Gas production, refining, treatment, storage and transmission by pipelines LNG terminals; • Transport: Road, rail, air, inland waterways, ocean and short-sea shipping and ports; • Additional sectors might be added with the review of the Directive. **Provisions on security requirements** The Directive sets security requirements for critical infrastructure: • Designation;	**MS** – here, including the owners/operators of ECIs that are 'primarily and ultimately responsible" for protecting ECI – are responsible for: • Identifying potential ECIs based on the criteria defined by the Directive; • Collecting information concerning ECIs in a MS's territory and inform the Commission on risks, threats and vulnerabilities of a sector; • Determining on a case-by-case basis the precise thresholds applicable to the cross-cutting criteria (each MS concerned by a particular critical infrastructure); • Ensuring that an operator security plan (OSP) or an equivalent measure is in place for each designated ECI to identify the existing security solutions for protecting them. The minimum content to be covered is defined in the Directive; • Appointing a ECIP contact point to coordinate with the Commission; • Appointing a Security Liaison Officers (or an equivalent), identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities; • Providing owners/operators with access to best-practice; • ensure coherent and secure information exchange in order to develop EU CI protection activities also in areas requiring confidentiality.

(Critical) infrastructure protection	
• security systems and procedures, taking into account sector specifities and existing sector based measures at regional, national and EU level. As for electricity production and transmission the Directive it is understood that electricity transmission may include parts of nuclear electricity generation but would exclude the particular nuclear elements covered by relevant legislation. **Provision on implementation mechanism** The Directive defines cross-cutting criteria to help MS designate ECIS: • casualties criterion (potential number of fatalities); • economic effect criterion (significance of economic loss); • public effect criterion (impact on public confidence, suffering, loss of essential services). The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure.	

Table 5.5 Border security: EU regulatory framework

Border security	
International legislation: not applicable (US unilaterally adopted biometric passports in 2002 and EU followed with Council Regulation Nr. 2252/2004)	
EU legislation	**National responsibility**
List of legislative acts Regulation (EC) No 562/2006 of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code). Regulation (EC) No 444/2009 of 28 May 2009 amending Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Decision of 28 June 2006 supplementing Regulation 2252/2004 by providing technical specifications relating to storage and protection of fingerprints to be integrated into passports and travel comments issued by MS. **Objectives** The Regulation is intended to improve the legislative part of the integrated border management policy by setting out the rules on crossing external borders and on reintroducing checks at internal borders. The Regulation on biometric has for objective to determine the biometric identifiers which will be introduced by MS with a view to harmonizing national legislation. Integration of biometrics in passports and travel documents also improves document security and prevent falsification of documents. **Means, scope** The Schengen Borders Code only covers those Member States who have signed the Schengen agreement. **Field of application** The Regulation applies to the integration of biometrics in passports and travel documents. **Provisions on Common basic rules** The Regulation sets minimum security standards of passports and travel documents issued by	**Schengen borders code** *External borders* Member States must deploy appropriate staff and resources in sufficient numbers to ensure a high and uniform level of control * at their external borders. They must ensure that border guards are specialised and properly trained professionals. Member States assist each other with the effective application of border controls. Operational cooperation is coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the EU Countries (FRONTEX). *Internal borders* Member States must remove all obstacles to fluid traffic flow at road crossing-points at internal borders. Where there is a serious threat to public policy or internal security, a Member State may exceptionally **reintroduce border controls** at its internal borders for, in principle, a limited period of no more than thirty days. If such controls are to be reintroduced, the other Member States and the Commission should be informed as soon as possible. The European Parliament should also be informed. Consultations take place between Member States and the Commission at least fifteen days before the planned date for the reintroduction of border controls, in order to organise mutual cooperation and to examine the proportionality of the measures to the events giving rise to the reintroduction. The decision to reintroduce border controls at internal borders must be taken in a transparent manner and the public must be informed in full, unless there are overriding security reasons for not doing so.

Border security	
the Member States : a. Material - the paper used for those sections of the passport or travel document giving personal particulars or other data shall meet minimum requirements; b. Biographical data page - the passport or travel document shall contain a machine-readable biographical data page; c. Printing techniques; d. Protection against copying; e. Issuing technique. **Provision on implementation mechanism** The technical specifications relating to storage and protection of fingerprints to be integrated into passports and travel documents issued by Member States addressing the following points: • primary biometric – face; • secondary biometric – fingerprints; • storage media; • electronic passport chip layout; • data security and integrity issues; • conformity assessment.	Under exceptional circumstances, the Member State concerned may reintroduce checks at its internal border immediately, if required by considerations of public order or national security. The other Member States and the Commission are then notified accordingly. **Biometric passports** Each Member State will designate one body for printing passports and travel documents. The Commission and the other Member States will be informed of the name of that body. Member States may at any time decide to confer that task on another body.

Table 5.6 Customs control (security): EU regulatory framework

Customs control	
International Legislation International Convention on mutual administrative assistance in Customs matters (Johannesburg Convention), June 2003	
EU Legislation	**National responsibility**
List of legislative acts Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code. Commission Regulation (EEC) No 2454/93 of 2 July 1993 laying down provisions for the implementation of Council Regulation (EEC) No2913/92 establishing the Community Customs Code . Regulation (EC) No 648/2005 of 13 April 2005 amending Regulation (EEC) No 2913/92 establishing the Community Customs Code. Regulation (EC) No 1875/2006 of 18 December 2006 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92. Regulation (EC) No 1875/2006 of 18 December 2006 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92. Regulation (EC) N°450/2008 of the European Parliament and of the Council of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code). **Objectives** The Community Customs Code compiles the rules, arrangements and procedures applicable to goods traded between the European Community (EC) and non-member countries. The Code is a single act covering the scope, definitions, basic provisions and content of Community customs law. In order to respond to security concerns relating to the international trade in goods, the European Commission adopted a series of measures designed to provide a coordinated and effective response. This package brings together the basic concepts underlying the new security-management model for the EU's external borders, such as a harmonized risk assessment system. It requires pre-arrival and pre-departure information (in the form of summary declarations lodged before the goods are brought into or out of the Community customs territory) to be filed electronically and also envisages exchange and sharing of the information between the Member States administrations, when possible. The Modernised Customs Code creates a new electronic customs environment. The new Code integrates the common customs procedures in the Member States while reinforcing convergence between the computerised systems of the 27 customs authorities. It will replace	Responsibilities include (taken from regulation on modernized customs code): • Maintain a regular dialogue with economic operators and other authorities involved in international trade in goods; • Promote transparency by making the customs legislation, general administrative rulings and application forms freely available, wherever practical without charge, and through the Internet; • Cooperate with the Commission with a view to developing, maintaining and employing electronic systems for the exchange of information between customs offices and for the common registration and maintenance of records; • Take decisions with regards to the application of customs regulations; • Apply penalties for failure to Community customs legislation; • Carry out customs controls in respect of the cabin and hold baggage of persons either taking an intra-Community flight, or making an intra-Community sea crossing, only where the customs legislation provides for such controls or formalities; • Carry out periodical checks of goods entering the Community.

Customs control	
the 1992 Customs Community Code, once the necessary implementing provisions are adopted and made applicable, at the latest by 24 June 2013. In the interim period the existing code applies. **Means, scope** The security amendment to the Community Customs Code (Regulation (EC) n° 648/2005 of 13 April 2005) introduces a number of measures to tighten security for goods crossing international borders. It will mean faster and better-targeted checks. **Field of application** The Security amendment covers three major changes to the Customs Code: • Requiring traders to provide customs authorities with information on goods prior to import to or export from the European Union; • Providing reliable traders with trade facilitation measures (Authorised Economic Operator (AEO)); • Introducing uniform Community risk -selection criteria for controls, supported by computerized systems. **Provision on implementation mechanism** The regulation also contains the implementing provisions for the Community Customs Code. It covers: • General implementing provisions; • Customs-approved treatments or uses; • Privileged operations; • Customs debt and certain controls. The implementing provisions set out the operational details in the customs processes for the above mentioned measures (see Regulation (EC) No 648/2005). They apply within the following timeframe: 1. Use of a common risk management framework to support improved risk based controls by customs authorities; 2. On 1 July 2009 it has became mandatory for traders to provide customs authorities with advance information on goods brought into, or out of, the customs territory of the European	

Customs control	
Union; 3. Entry into force, on 1 January 2008, of the provisions for the Authorised Economic Operator programme (AEO).	

Table 5.7 Export controls (security): EU regulatory framework

Export Controls	
International legislation International export control regimes – the Australia Group (AG), the Nuclear Suppliers Group (NSG), the Wassenaar Arrangement and the Missile Technology Control Regime (MTCR).	
EU Legislation	**National responsibility**
List of EU legislation Regulation (EC) No 1334/2000of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology. **Objective** The Regulation establishes a regime for controlling the export, transfer, brokering and transit of dual-use items. **Means, scope** Certain items which require to be controlled under the EU Regime may not leave the EU customs territory without an export authorisation. Additional restrictions are also in place concerning the provision of brokering services with regards to those items and concerning the transit of such items through the EU. **Field of application** An authorization is necessary for the export of: • Dual-use items listed in the Regulation and (the EU list of controlled items is based on control lists adopted by international export control regimes). Any products, software or technology that can be used for both civil and military purposes are considered to be dual-use items; • In case an exporter has been informed by the competent authorities of the EU country in which he is established that the items in question are or may be intended, in their entirety or in part, for use in connection with: - The development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices; - The development, production, maintenance or storage of missiles capable of delivering	If an exporter is aware that the items in question, not listed in Annex I, are intended for any of the above listed uses, he must inform the relevant competent national authorities which will then decide whether an authorisation is necessary for the export concerned. These brokering controls can be extended under national legislation to also cover other situations. An EU country may introduce additional national legislation to prohibit or impose an authorisation requirement for dual-use items not listed in Annex I for reasons of public security or human rights considerations. MS in which the exporter is established is responsible for granting any other export authorization. If an export might prejudice its essential security interests, a MS may request another MS not to grant an export authorization or to annul, suspend, modify or revoke it. In such cases, the two MS are to consult with each other immediately. A MS may provisionally suspend the process of export from its territory if it suspects that important information was not been taken into account when the authorization was granted or that circumstances have materially changed.

such weapons;
- a military end-use and the purchasing country or country of destination is subject to an arms embargo;
- use as parts or components of military items that have been exported from the EU without authorization or in violation of an authorization;
- development of weapons of mass destruction or their means of delivery.

- If the broker is aware that the items are or may be intended for these uses, he must inform the national authorities.

Provision on export control

The export of dual-use items listed in the Regulation is subject to authorization. The authorization is valid throughout the EU.

A general Community export authorization has been set up for certain categories of products destined for the following countries: Australia, Canada, Japan, New Zealand, Norway, Switzerland, US.

Table 5.8 Data protection (security): EU regulatory framework

Data protection	
International legislation: Terrorist Financing Tracking Programme (TFTP) EU-US International Agreement on the processing and transfer of financial data	
EU legislation	**National responsibility**
List of legislative acts Charter of Fundamental Rights of the European Union. European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR): Art. 8. Consolidated Version of the Treaty on the Functioning of the European Union (TFEU): Art. 16. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. **Objectives** The Data Protection Directive applies to protection of individuals with regard to the processing of personal data and on the free movement of such data; **Means, scope** The Directive defines personal data as “any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.	Member States must: • Establish supervisory authorities to monitor respect of privacy in the collection and processing of data; • Provide that data is processed fairly and lawfully, for specified and legitimate purposes, and that it is proportional to the requirements of the controller. It should be kept in a manner which allows deletion after use and accuracy during use; • Ensure that data is only processed if the requirements of the Directive are met; • Prohibit the processing of certain sensitive types of personal data (e.g. racial origin); • Ensure the data controllers can provide data subjects with data currently held and the intended use of data to potential new data subjects; • Ensure that data subjects can object to the use of the data and are aware of this right; • Ensure that controllers put in place sufficient safeguards to avoid the accidental loss of data; • Ensure that data controllers notify the supervisory authorities when automatically collecting data; • Examine procedures that present particular risks to privacy; • Take measures to ensure processing operations are publicised; • Provide the right to a judicial remedy and compensation; • Adopt measures to ensure the implementation of the Directive, including sanctions; • Regulate the transfer of data to third countries according to the Directive; • Encourage the drawing up of codes of conduct.

Data protection	
The Directive covers most sectors apart from those related to security and defence or criminal matters. Not all data can be processed (e.g. religious belief or political affiliation). **Field of application** The Directive applies to data processed by automated means (e.g.) a computer database of customers) and data contained in or intended to be part of non automated filing systems (traditional paper files). It does not apply to the processing of data by a natural person in the course of purely personal activities or in case of operations concerning the public security, defence or State security.	

5.5 European case-law of relevance to the security market

This sub-section looks at case law from the European Court of Justice (ECJ) relevant to security products. Case law that is more related to the issue of (notification of) technical regulations is addressed in Section 1. A summary of selected case law is provided in Table 5.9 .

The main area of relevant ECJ case law appears to relate to the interpretation of Article 296 of the Treaty establishing the European Community (TEC) – currently Article 346 of the Treaty on the Functioning of the European Union (TFEU) – which allows Member States to derogate from Internal Market rules when their essential security interests are at stake. The national security exemption provides that a Member States is not obliged to supply information the disclosure of which it considers contrary to the essential interests of its security. Further, a Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material.

In 2006, the Commission issued a Communication setting out its own views on the principles governing the application of Article 296 and explain its understanding of the conditions for the application of the derogation in the light of the ECJ case law.[74] Subsequently, the 2009 Defence Procurement Directive75 sought to open up defence - and sensitive security equipment - markets to competition and to contribute to development of an efficient European market. However, given the precedence of Article 346 (TFEU) over the Directive, the principles laid down by the ECJ (and the Commission Communication) retain their relevance.

Briefly, the ECJ has ruled that the derogations from the Treaty provisions offered by the Article(s) must be interpreted strictly, thus requiring Member States to fulfil stringent requirements in order to be able to rely on the exemption (see Table 5.9). However, EUISS (2008)[76] notes the relative absence of case law in relation to the interpretation of Article 296 TEC (now Article 346 TFEU), implying that "*the law is unclear, because there simply have not been enough cases*". In the context of this study, the lack of clarity is of particular relevance with regard to the extent to which the Article applies to security 'products', and in particular dual-use products[77], that are not purely defence products. The Article makes reference to the so-called '1958 list' of military equipment but this list is in itself open to interpretation. Thus, while the ECJ has confirmed that the concept of public security within the meaning of this Article covers a Member State's external and internal security, there is a lack of clarity as to which categories of security products fall within the scope of TEC Article 296 / TFEU Article 346. Similarly, there is a lack of clarity as to which products with security implications, such as those with dual-uses, fall within the scope the common commercial policy (Article 207 TFEU). This assessment will determine the existence or absence of EU exclusive competence on their regulation. This field's legal framework has become all the more complex with the expansion of ICT and the increasing securitization of our societies.

The booming and widespread use of ICT, and the monitoring and surveillance technology that stems from it, have opened an unchartered area for which delicate balances need to be struck between the rights of the individuals to privacy and the security interests of the state. Both the ECJ

---

74 COM (2006) 779: Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement.

75 Directive 2009/81/EC of 13 July 2009 on the coordination of procedures for the award of public contracts in the fields of defence and security.

76 European Union Institute for Security Studies (2008) 'Towards a European Defence Market' Chaillot Paper No. 113, November 2008.

77 This lack of clarity may be extended not only to other sensitive and military equipment not explicitly listed but, also to other areas such as construction contracts and service contracts.

and the ECHR have acknowledged this need in their extensive jurisprudence and have responded by developing certain legal tests for such balancing act. The EU institutions have followed suit with the adoption of regulations such as the personal data protection Directive 95/46/EC and the privacy and electronic communications Directive 2002/58/EC that complements it. These Directives are nowadays the main EU regulatory instruments in this field. Since their adoption, the ECJ has clarified and developed their content, mostly expanding the rights of the individuals and limiting the prerogatives of the states. The ECJ has thereby promoted the right to know to whom personal data has been disclosed and to have access to its content. It has ruled on data retention time periods and ensured that it was collected, stored and used in a fair and non-discriminatory manner. At the same time, it has defended the EU's competences in this field and ruled against those states which did not ensure the independence of supervisory data protection authorities. Furthermore, the scope of these Directives was left open-ended, allowing Member States to expand it through their national implementing legislation. This leads to divergences among Member States in the level of data protection that can affect to the commercialisation and use in Europe of ICT-based security products and monitoring and surveillance technology.

Table 5.9 Selected case law from the European Court of Justice of relevance for security products

Field	Reference	Rule of law
Use of Derogations to the Treaty Provisions on security grounds	Judgment of 16 September 1999, Case C-414/97 *Commission v Spain* Judgment of 15 May 1986, Case C-222/84 *Johnston*	Article 296 of the TEC – currently article 346 TFEU - allows Member States certain derogations from the Treaty Provisions in cases where they consider it necessary for the protection of their "**essential interests of its security**" connected to the supply of information, or the production of, or trade in arms, munitions and war material. The **products covered must be intended for specifically military purposes**. These arms, munitions and war material are included in a list, foreseen in paragraph 2 of the same article. **VAT exemptions cannot be considered necessary** for the protection of essential security interests. The ECJ underlined that these cases must be **clearly defined and exceptional**. Because of their limited character, the Article(s) must be interpreted strictly. The derogation cannot go beyond the limits of such cases. The **burden of proof** on the "clearly defined" and "necessary for the protection of the essential interests of its security" character **falls on the Member State** using the derogation.
	Judgment of 30 September 2003, Case T-26/01 *Fiocchi Munizioni v Commission*	The derogations to the Treaty provisions foreseen in Article 296 can **only cover activities related to arms, munitions and war material** included in the updated 15 April 1958 list mentioned in paragraph 2 of the article.
	Judgment of 26 October 1999, Case C-273/97 *Sirdar* Judgment of 11 January 2000, Case285/98 *Kreil* Judgment of 11 March 2003, Case C-186/01 *Dory*	The possibility of **certain derogations provided by Article 296 is only applicable to exceptional and clearly defined cases**. It cannot be considered a general exception covering all measures taken for reasons of public security. The concept of **public security** within the meaning of this Article **covers a Member State's external and internal security**. This derogation concerns the **rules relating to the free movement of goods, persons and services**.

Field	Reference	Rule of law
	Judgment of 13 July 2000, Case C-423/98 *Albore*	**Derogations on the grounds of public security must observe the principle of proportionality** to be valid, i.e. that the derogation remains within the limits of what is appropriate and necessary for achieving the aim in view.
	Judgment of 15 December 2009, Case C-372/05, see cases C-490/05, +C-141/07, *Commission* v. *Germany* Judgment of 15 December 2009, C-294/05, *Commission* v. *Sweden* Judgment of 4 March 2010, C-38/06, *Commission* v. *Portugal* Judgment of 26 June 2008, C-284/06, *Commission* v. *Finland* Judgment of 15 December 2009, C-409/05, *Commission* v. *Greece* Judgment of 15 December 2009, C-461/05, *Commission* v. *Denmark* Judgment of 15 December 2009,C-239/06, see also 387/05, *Commission* v. *Italy*	The Court **rejects the exemption of imports of military equipment from custom duties** and the absence of a declaration to the Commission **on the grounds of special security interests** – Article 346 TFEU. The Court holds that notwithstanding the provisions in the Article allowing for a derogation, it cannot be read in such a way as to confer on Member States a power to depart from the provisions of the Treaty based on no more than reliance on those interests. The implementation of the **Community Customs system** requires the active involvement of Community and national officials **including the imports and acquisitions of arms, ammunition and equipment exclusively for military use**. The Court bases also its rulings on the previously-mentioned case-law concerning this issue.
Criminal law	Judgment of 13 September 2005, Case C 176/03, *Commission v Council*	The **choice of the legal basis for a Community measure must rest on objective factors** which can be subject to judicial review, including in particular the aim and the content of the measure. The European Union legislature can require to the competent national authorities to adopt measures related to criminal law when it is necessary for the effective implementation of Community law. These measures must be consistent with the Union's system of criminal law.[78]
Trade in dual-use goods and export controls	Judgment of 17 October 1995, Case C-70/94, *Werner* Judgment of 17 October 1995, Case C-83/94, *Leifer*	**A measure ( ) whose effect is to prevent or restrict the export of certain products falls inside the scope of the common commercial policy, even if it was adopted on foreign policy grounds and security objectives**. The fact that "a trade measure may have non-trade objectives does not alter the trade nature of such measures". The EU has therefore exclusive competence in this matter, excluding that of the states except on those cases where the EU grants

[78] In the future, the EU could accede to security-related international conventions touching upon matters under its competence, such as trade of dual-use goods or dangerous substances. It would therefore be competent under this ECJ ruling to require its Member States to adopt criminal provisions needed to enforce effectively such conventions.

Field	Reference	Rule of law
		them specific authorization. The concept of common commercial policy contained in article 133 CE –currently Article 207 TFEU - cannot be interpreted in a strict manner. **The nature of dual-use goods does not exclude them from the common commercial policy.**
Data protection and privacy	Judgment of 9 March 2010, Case C-518/07, *Commission v. Germany*	The **independence of supervisory data protection authorities is an essential element** in light of the objectives of Directive 95/46 and is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data. The requirement of independence goes beyond the relationship between the supervisory authorities and the bodies subject to that supervision. "**Complete independence"** as prescribed in the Directive, entails a **decision-making power independent of any direct or indirect external influence on the supervisory authority.** The **supervisory data protection authorities cannot be subject to State scrutiny**, as they must perform their functions with complete independence.
	Judgment of 7 May 2009, Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer*	Article 12 (a) of Directive 95/46/EC requires **Member States to ensure a right of access to information on the recipients of personal data and on the content of the data disclosed in the past and in the present**. States can fix a **time-limit** for the **storage** of such information and provide **access** to it, striking a **fair balance** between the **interests and rights of the affected** party and the **needs of the controller**. Rules limiting this storage to a period of one year, while basic data is stored for a much longer period, are against this balance. Unless it can be shown that these limitations are necessary. It is for national courts to make the necessary determinations.
	Judgment of 16 December 2008, Case C-524/06, *Huber v. Germany*	A **system for processing of personal data relating to Union citizens non-nationals of the Member State** concerned does not satisfy the requirement of necessity of Article 7(e) of Directive 95/46/EC, and **is** therefore **an unlawful discrimination on the grounds of nationality. It will only fulfil the necessity requirement if the data is necessary for the application by the authorities of legislation relating to the right of residence and if its centralised nature enables such legislation to be more effectively applied to EU citizens not nationals of that Member State.** It will correspond to the national court to determine if these conditions are satisfied.
	Judgment of 10 February 2009, Case C-301/06, *Ireland v. Parliament and Council*	**Directive 2006/24 on the retention of electronic communication data** falls within **EU's competence** in regulating the functioning of the **internal market**, as provided in former **article 95 of the EC Treaty** –currently article 114 TFEU-. The impact on the functioning of the

Field	Reference	Rule of law
		internal market that could derive from differences between various national rules concerning the retention of data justified the Community's adoption of rules in this field. Thus, this field falls within the Community Powers. **Directive 2006/24 covers activities of service providers and does not contain rules concerning law enforcement activities of public authorities.**
	Judgment of 30 May 2006, Cases 317/04-318/04, *Parliament v. Council (PNR)*	The **transfer of Passenger Name Records** to an authority such as the U.S. Bureau of Customs and Border Protection is a **processing operation that relates to public security and the activities of the State in areas of criminal law**. It cannot then be considered that the data processing is needed for a supply of services, which would be covered by Community law -Article 95 TEC, currently article 114 TFEU-. **These activities do not fall therefore under the Community Competence.**
	Judgment of 6 November 2003, Case C-101/01, *Lindqvist,*	**Directive 95/46** intends **to ensure** that the **level of protection** of the rights and freedoms of individuals with regard to their **personal data** is **equivalent in all Member States.** **Member States can extend the scope of the national legislation implementing the provisions of Directive 95/46 to areas not covered by the latter**, unless some other EU law provision precludes this. The applicability of Directive 95/46 does not depend on whether each situation is sufficiently linked to fundamental freedoms provided in the EU Treaties such as freedom of workers.
	Judgment of 20 May 2003, Case 465/00 and Case 138/01, *Rechnungshof v. Osterriechischer Rundfunk*	The **provisions of Directive 95/46** must be **interpreted in the light of the right to privacy**, which is an integral part of the general principles of Community law**. Public authorities cannot interfere with the right to private life** of the European Convention of Human Rights –Article 8 ECHR- **unless** they do so **in accordance with the law** and because it is **necessary in a democratic society to protect certain interests**. The **articles 6(1) (c) and 7(c) and (e) of the Data Protection Directive are directly applicable**, i.e. an individual may rely on them before national courts against a national rule that is contrary to them.
	Judgment of 4 December 2008, Case ECHR 880, *S. and Marper v. the United Kingdom*	The **use of modern scientific techniques in the criminal-justice system cannot be allowed at any cost** and **without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests**. **Otherwise**, the **protection of the right to privacy** afforded by Article 8 of the ECHR would be **unacceptably weakene**d. Any state with a pioneer role in the development of new technologies bears special responsibility in striking a balance in this regard.

Field	Reference	Rule of law
	Judgment of 28 April 2003, Case ECHR 44647/98, *Peck v. United Kingdom*	To **determine whether a particular disclosure of CCTV images is "necessary in a democratic society"** the European Court of Human Rights will **consider whether the reasons justifying such disclosure were relevant, sufficient, and proportionate to the legitimate aims pursued.** In **cases concerning disclosure of personal data** the **margin of appreciation** of **the fair balance between relevant public and private interests should be left to the competent national authorities**. This margin of appreciation can be **accompanied by European supervision and its scope will depend on factors such as the nature and seriousness of the interests at stake and the gravity of the interference.**
	Judgment of 6 September 1978, Case ECHR 5029/71, *Klass and others v. German*	**Democratic societies must be able to undertake secret surveillance** of subversive elements operating within its jurisdiction **to counter the threats of terrorism and espionage** they face. Nevertheless, **states may not** in the name of this struggle **adopt whatever measures they deem appropriate.**

6 EU regulatory framework for notification of product-related technical regulations

6.1 The 98/34 notification procedure[79]

The 98/34 notification procedure is a mechanism through which Member States are obliged to notify the Commission of their draft technical regulations related to products[80] and Information Society services before they are adopted in to national law. The relevant legal texts are:

- **Directive 98/34/EC**[81] of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations formerly 83/189/EC);
- **Directive 98/48/EC** of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC.

The 98/34 procedure aims to provide transparency concerning national initiatives establishing technical standards or regulations, thereby providing an opportunity – for the Commission, Member States and other stakeholders/public – to evaluate whether such regulations may create an unjustified barrier between Member States. Accordingly, their notification in the draft form and subsequent evaluation of their content in the course of the procedure aim to diminish this risk.

The notified drafts and their translations in all EU languages are communicated to the Member States and are available to the public on the TRIS (Technical Regulations Information System) database. The Commission and the other Member States can react in specific forms if the draft appears incompatible with EU law or if its quality could be improved. Economic operators (e.g. enterprises, industry associations) have the possibility to communicate to the Member States and to the European Commission their concerns on a given notified draft; position papers sent within the 'standstill period' (normally 3 months) should be taken into account during the analysis of the notified draft.

While it is not the purpose of this report to provide a detailed description or assessment of the notification procedure, some points of relevance for the present study are as follows:
The notification provisions cover draft technical regulations that apply to:

- **Industrial manufactured (or agricultural) products**;
- **Services provided on a commercial basis over the internet** or through any similar medium (referred to as 'Information Society services').

---

79 A useful guide to the 98/34 notification procedure is provided by the UK Department for Business, Innovation and Skills (BIS) at: http://www.bis.gov.uk/policies/innovation/standardisation/tech-standards-directive/98-34-at-a-glance#techanchTOP. See also:
UK Department for Business, Innovation and Skills (BIS) "Guidance for officials: avoiding new barriers to trade, Directive (as amended by Directive 98/48/EC)", available at: http://www.bis.gov.uk/assets/biscore/corporate/docs/a/02-1434-avoiding-new-barriers-to-trade.pdf;
European Commission (2008) "Preventing obstacles to trade in the internal market: Directive 98/34/EC", available at: http://ec.europa.eu/enterprise/policies/single-market-goods/files/brochure-preventing/index_en.pdf.
European Commission index of relevant case law, available at http://ec.europa.eu/enterprise/tris/case_law/index_en.htm.

80 The Directive covers all agricultural and information society services.

81 As amended by Directive 88/189/EC.

NB. The Commission view is that the "*Directive draws no distinction on the basis of the value of the products, size of the market etc. and contains no de minimus rule. Consequently, rules applying to products not in common use or with a negligible economic impact must be notified*"[82].

> **Case C-226/97 *Lemmens:*** the European Court of Justice (EJC) confirmed that there were no exclusions from the definition of product. In that case Member States had sought to argue that products connected with the criminal law (in that case a breathalyser) were excluded from the scope of the notification requirements and that the directive only applied to 'everyday products'. The court rejected this argument (paras. 23-24). The Court referred to **Case C-13/96 *Bic Benelux*** where the ECJ ruled that the grounds on which a technical regulation was adopted was irrelevant to the issue of whether there was a requirement to notify them in draft.[83]
>
> Note, this case establishes that where technical specifications must be complied with for sales to a particular group of users / a major user on the market in question, they are technical regulations.

The notification provisions relate to national 'technical regulations' (see below) of Member States. This covers regulations laid down by central government, including agencies or other bodies responsible for technical regulations which apply nationally in a Member State or a significant part of that State; consequently, relevant authorities may also include regional-level authorities[84].

The scope of 'technical regulations' is given a broad meaning, such that the types of rules to be notified include prohibitions, technical specification and 'other requirements' affecting the life-cycle of a product (e.g. condition of use, recycling, reuse, disposal).

> Case C-194/94, CIA Security International SA v Signalson SA and Securitel SPRL: the European Court of Justice (EJC) ruled that:
>
> - A rule can be considered a technical regulation for the purposes of Directive 83/189[85] if it has legal effects of its own. If, under domestic law, the rule merely serves as a basis for enabling administrative regulations containing rules binding on interested parties to be adopted, so that by itself it has no legal effect for individuals, the rule does not constitute a technical regulation within the meaning of the Directive;
> - A rule must be classified as a technical regulation within the meaning of Directive 83/189 if it requires the undertakings concerned to apply for prior approval of their equipment, even if the administrative rules envisaged have not been adopted;
> - A rule on caretaking firms, security firms and internal caretaking services laying down a procedure for the provision of information in the field of technical standards and regulations is not a technical regulation within the meaning the Directive, whereas provisions laying down the procedure for approval of the alarm systems and networks are technical regulations.

The notification provisions may cover a technical specification or standard drawn up by national standards institutions where these are made on the request of public authorities for the purpose of enacting a technical regulation for a product the draft of which is, itself, notifiable. National standards, which by definition are drawn up by private bodies and are in essence

---

82 Commission Working Paper "The 98/34 Notification Procedure Working Paper: Court of Justice Judgements and Commission Practice", as quoted by BIS (Ibid. footnote 79). The link to the Working Paper on the Commission website is broken.

83 Ibid. footnote 79.

84 The relevant authorities are specified in a list drawn up by the Commission in the framework of the Standing Committee of the Directive. See List: http://ec.europa.eu/enterprise/tris/who/c_12720060531en00140015.pdf.

85 Directive 98/34/EC is a codification of Directive 83/189/EC, as amended.

voluntary, are not in themselves notifiable. However, where compliance with a standard becomes 'compulsory' (see next point) then it falls within the scope of the notification provisions.

- ***De jure* and *de facto* rules are covered.** The scope of technical regulations includes primary and secondary legislation that create *de jure* obligations and, also, other documents – such as administrative circulars, departmental guidelines, advice notes, codes of practice, voluntary agreements, etc. – that recommend the use of given specifications or standards such that compliance with the specifications or standards is *de facto* obligatory. In this respect, European Commission (2005) notes:
  - The laws, regulations or administrative provisions referred to are measures adopted by the national authorities which refer to technical specifications or 'other requirements' or to rules on services usually laid down by bodies other than the State (by a national standardisation body, for example), which are not compulsory as such (standards, professional codes or codes of practice), but observance of which is encouraged since it confers on the product or the service a presumption of conformity with the provisions of the aforementioned measures;
  - Agreements entered into between economic operators which establish technical specifications or other requirements for certain products or rules on services are not binding as such owing to their origin in the private sector. They are nevertheless considered to be *de facto* technical regulations when the State is a signatory party to one of these agreements.
- **Testing and test methods to be used to evaluate the characteristics of products, together with conformity assessment procedures used to ensure that a product conforms to specific requirements are covered** within the scope of 'draft technical regulations'. The inclusion of these parameters reflects recognition that testing and conformity assessment procedures can, under certain conditions, have negative effects on trade. The multiplicity and disparity of national systems of conformity certification can cause technical barriers to trade in the same way as specification applicable to products, which are even more difficult to overcome as a result of their complexity;[86]
- **Member States may introduce and enact technical regulations without observing the Directive's 'standstill requirements' for urgent reasons**, occasioned by serious and unforeseeable circumstances. This provision provides that the standstill periods are not applicable when a Member State, in order to respond to an urgent and unforeseeable situation such as, for example, a natural disaster (the need to protect people, the atmosphere, soil or water), an epidemic, an animal epidemic, etc., is obliged to prepare technical regulations for immediate introduction, without having time to consult the Commission and the other Member States beforehand. These exceptional circumstances do not exempt the Member State from the obligation to inform the Commission of the planned measures and clearly justify its request for urgency at the time when the text is communicated;
- **Members States are not obliged to notify draft technical regulations which fulfil obligations arising out of Community measures, or that fulfil obligations arising out of international agreements** (which all Member States are party to) and which result in the adoption of uniform technical specifications in the EU.

[86] European Commission (2005) "A guide to the procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services", available at: http://ec.europa.eu/enterprise/tris/info_brochure/2003_2121_EN.pdf.

6.2 Assessment of security-related technical regulations included in the TRIS database

The following assessment is based on a 'key-word'[87] search of the TRIS database for the last decade[88]. This identified 121 notifications draft technical regulations that appear to be related to security (as understood in the context of this study). It should be noted, however, that:

- A single notification may cover a number of different categories of security products or services;
- Multiple notifications may result from a single legislative instrument (or other document);
- Both original notification and subsequent revisions to 'draft' technical regulations are included in the total indicated above.

Table 6.1 provides an overview of the number of identified notifications by Member State and by 'category'; with regard to the categories indicated, there is no standard nomenclature applied in the TRIS database and so the categories shown are only indicative. The identified notifications are listed in Table 6.2 .

As a first point it may be noted that notifications related to security are identified for only 19 Member States. The main categories of notifications are as follows:

- The category with the highest frequency of notifications is labelled under the generic heading of 'Data protection 1'. These are primarily regulations related to security of electronic transactions and data transmissions (e.g. electronic signatures, security/identity certification) and, also, in relation to other forms of identification/authentication (e.g. identity cards, biometric data). The second category, 'Data protection 2' covers, in particular, regulations relating to the activities of telecommunications and related service providers and requirements to retain (and make available) information of telecommunication and internet traffic (e.g. where such information may be required by government intelligence/security services). This is also relevant for the category of 'Telecommunications equipment', where this concerns technical regulations related to equipment used for the purposes of intercepting telecommunications transmissions;
- Five countries have provided notifications relating to regulations setting technical requirements for equipment used by private security services personnel but also includes alarm monitoring services;[89,90]
- A few countries have notified regulations in relation to weapons (primarily in relations to firearms) and chemical substances (explosives and chemical weapons).

Leaving aside the aforementioned categories, the general picture is of very few notifications of national regulations relating to security products of relevance in the context of the present study. There is no evidence across countries (or even within countries) that would indicate general patterns in the development of technical regulations related to security products. Overall, with the exception of IT security-related technical requirements, the analysis of TRIS notifications points to a general absence in the development of national frameworks for concerning technical requirements/specifications for security products (de jure or de facto).

---

87 The 'key-word' search primarily identified draft technical regulations containing the term 'security', other 'key-words' reflecting the main economic sectors covered by the study (e.g. aviation/airports, maritime/ports, urban transport) and relevant equipment and technologies (e.g. alarm, biometric) were also used.

88 Data extracted on 17 June 2011.

89 As a passing observation it is not clear if such an activity falls within the definition of an 'Information Society service'.

90 This also appears relevant for the category 'Vehicles (transport of valuables)' as this is an activity undertake by private security service providers; information on the Belgian notifications for this category are confidential.

In assessing the above, it can be noted that the TRIS database is limited to technical regulations at national level (and 'larger' sub-national authorities[91]), while responsibilities for specification of requirements and procurement are often at a local-level or, as a result of privatisation, have shifted from the public to private sector. Thus, the absence of TRIS notifications would seem to accord with the general perception that weak (national) regulatory frameworks for many categories of security equipment – and corresponding standards and conformity assessment and approval/certification procedures – contribute to market fragmentation.

[91] Ibid. footnote 84.

Table 6.1 Overview of TRIS notifications of draft technical regulations related to security by Member State (2001-2011)

	Data-protection 1 (identification, electronic signatures, identity certification)	Data-protection 2 (telecommunication services, data storage, data transmission)	Telecommunications equipment	Telecommunications (emergency services)	Private security services	Private security services / Alarm systems	Vehicles (transport of valuables)	Dual-use (services)	Dual-use	Dual-use (biological substances)	Chemicals (weapons, explosives)	Nuclear Facilities	Radioactive detection equipment	Weapons	Police / Fire Service equipment	Protective clothing	Vehicles	Alarm Systems	Surveillance (persons)	Surveillance (vehicles)	Physical security	Compliance assessment defence and security articles	**Total**	**Non zero**
Germany	**5**	**2**	**7**																				**14**	*3*
France	**5**																						**5**	*1*
United Kingdom	**1**								**1**														**2**	*2*
Italy	**7**																						**7**	*1*
The Netherlands	**1**	**5**	**1**	**2**				**1**				**2**	**2**		**1**			**1**					**16**	*9*
Poland															**2**	**1**	**1**		**1**			**2**	**7**	*5*
Sweden					**2**						**1**			**2**									**5**	*3*
Belgium	**3**	**1**			**2**		**8**							**1**					**2**				**17**	*6*
Spain	**2**				**4**													1					**7**	*3*
Latvia			**2**		**2**																		**4**	*2*
Slovenia		**2**									**1**												**3**	*2*
Romania						**1**																	**1**	*1*
Finland	**6**																						**6**	*1*
Denmark	**7**									**1**	**1**			**1**									**10**	*4*
Slovakia	**6**													**1**							**2**		**9**	*3*
Hungary														**1**						**1**			**2**	*2*
Austria	**2**																				**1**		**3**	*2*
Czech Republic	**1**										**1**												**2**	*2*
Portugal	**1**																						**1**	*1*
Total	**47**	**10**	**10**	**2**	**10**	**1**	**8**	**1**	**1**	**1**	**4**	**2**	**2**	**6**	**3**	**1**	**1**	**2**	**3**	**1**	**3**	**2**	**121**	
Non-zero	*13*	*4*	*3*	*1*	*4*	*1*	*1*	*1*	*1*	*1*	*4*	*1*	*1*	*5*	*2*	*1*	*1*	*2*	*2*	*1*	*2*	*1*		

Source: Ecorys based on TRIS database.

Table 6.2 TRIS notifications of draft technical regulations related to security by Member State (2001-2011)[92]

	Country	Reference	Category	Title
1	Netherlands	2011/112/NL	Dual-use (services)	Rules for monitoring services related to strategic items (Strategic Services Act).
2	Denmark	2011/109/DK	Weapons	Order on the amendment of the Order on Weapons and Ammunition etc.
3	Poland	2011/71/PL	Vehicles	Regulation of the Ministers for: the Interior and Administration, National Defence, Finances and Justice on the technical conditions of special vehicles and vehicles for the special purposes of the Police, Internal Security Agency, Intelligence Agency, Military Counter-Intelligence Services, Military Intelligence Services, Central Anticorruption Bureau, Border Guard, Tax Inspection, Customs Service, Prison Services and Fire Brigade.
4	Belgium	2010/805/B	Vehicles (transport of valuables)	The Royal Decree modifying the Royal Decree of 7 April 2003 on specific surveillance and protection methods for transporting securities and on the technical specifications of vehicles transporting securities.
5	Belgium	2010/746/B	Data protection 1	Articles 38 to 52 of the draft of the act to amendment of the act of 21 March 1991 on the reform of some economic public sectors, regarding the amendment of the act of 17 January 2003 with regard to the statute of the regulator of the Belgian post and telecommunication sector and to amendment of the act of 9 July 2001 regarding the determination of specific regulations in relation to the legal framework for electronic signatures and certification services. The involved articles bring amendments to the act of 9 July 2001 regarding the determination of specific regulations in relation to the legal framework for electronic signatures and certification services.
6	Spain	2010/620/E	Alarm systems	Draft Order of the Ministry of Interior on the performance of Private Security alarm systems.
7	Spain	2010/619/E	Private security services	Draft Order of the Interior Ministry on Private Security Personnel.
8	Spain	2010/614/E	Private security services	Draft Order of the Ministry of the Interior on Private Security Firms.
9	Spain	2010/613/E	Private security services	Draft Order of the Ministry of the Interior on Private Security Measures.
10	Poland	2010/582/PL	Surveillance (persons)	The Regulation of the Minister of the Interior and Administration of .... on the manner of recording mass events.
11	Netherlands	2010/498/NL	Nuclear Facilities	Regulation of the Minister for Housing, Spatial Planning and Environmental Management laying down rules with regard to the security of nuclear establishments and nuclear fuels (Nuclear Facilities and Nuclear Fuels Security Regulation, Regeling beveiliging nucleaire inrichtingen en splijtstoffen).
12	Poland	2010/332/PL	Police / Fire Service	Regulation of the Minister for the Interior and Administration of amending the Regulation on the specific manner of

[92] Data extracted on 17 June 2011.

	Country	Reference	Category	Title
			equipment	assessing the conformity of articles for the needs of State defence and security and a list thereof.
13	Italy	2010/305/I	Data protection 1	Draft decree of the Minister for Public Administration and Innovation, together with the Minister for Economic Development, concerning: “Technological means to guarantee the security, integrity and certification of electronic document transmission bearing an electronic postmark”.
14	Belgium	2010/262/B	Vehicles (transport of valuables)	Ministerial order setting out the methods for packaging banknotes in containers fitted with neutralisation systems.
15	Germany	2010/238/D	Data protection 1	Regulation on personal identification cards and electronic proof of identy (Personal Identification Regulation [Personalausweisverordnung – PAuswV).
16	Italy	2010/85/I	Data protection 1	Technical and security requirements for identification documents issued by State administrations.
17	Latvia	2010/9/LV	Telecommunications equipment	Cabinet of Ministers draft regulation “Procedure for the use and technical operating requirements of special radio devices”
18	Latvia	2010/8/LV	Telecommunications equipment	The Cabinet of Ministers draft regulation “Amendments to the Cabinet of Ministers regulation No 561 of 21 August 2007 “Procedure for the evaluation of compliance, marketing and use of radio equipment and telecommunication network terminals”.
19	Poland	2010/3/PL	Compliance assessment defence and security articles	Act amending the System of Compliance Assessment of Articles for the Needs of State Defence and Security Act of 17 November 2006.
20	Poland	2009/461/PL	Police / Fire Service equipment	Regulation of the Minister of the Interior and Administration of 2009 amending the Regulation on the list of products used for ensuring public security or protecting health, life and property, and the principles of issuing permission to use these products (draft of 17 August 2009).
21	Germany	2009/436/D	Telecommunications equipment	Technical Directive concerning the implementation of statutory measures for the interception of telecommunications and for traffic data enquiries (TR TKÜV), edition 6.0.
22	Italy	2009/411/I	Data protection 1	Rules for acknowledging and verifying electronic documents.
23	Sweden	2009/402/S	Private security services	The National Police Board’s regulations and general recommendations on the appointment of maritime and port security officers, RPSFS 2009:xx, FAP 699.1.
24	Denmark	2009/350/DK	Dual-use (biological substances)	Executive Order on securing specific biological substances, delivery systems and related materials.
25	Slovenia	2009/319/SI	Data protection 2	Rules on the method of transmission of retained data in fixed and mobile electronic communications network telephony services.

	Country	Reference	Category	Title
26	Romania	2009/280/RO	Private security services Alarm systems	Draft law for the modification and supplementation of Law no. 333/2003 on the guarding of facilities, goods and valuables, and the protection of people.
27	Finland	2009/140/FIN	Data protection 1	Law on strong electronic authentication and electronic signatures.
28	Germany	2009/76/D	Data protection 1	Law regulating citizen portals and amending further regulations, here Art. 1 Citizen Portal Act.
29	Netherlands	2009/55/NL	Nuclear Facilities	Regulation of the Minister for Housing, Spatial Planning and the Environment, containing rules on the protection of nuclear plants, fissile materials and ores (Nuclear Energy Act Protection Regulation).
30	Slovakia	2009/19/SK	Weapons	Government Ordinance of the Slovak Republic of .2008 amending and supplementing Government Ordinance of the Slovak Republic no. 397/1999 Coll. establishing details on the technical requirements and procedures of conformity assessment for firearms and ammunition as amended by the most recent legislation.
31	France	2008/599/F	Data protection 1	Order of on the General Security Framework.
32	Germany	2008/575/D	Data protection 1	Draft law regulating the data protection audit and amending data protection regulations.
33	Slovakia	2008/533/SK	Data protection 1	The draft decree of the National Security Agency on the method and procedure of using the electronic signature in commercial and administrative affairs.
34	Slovakia	2008/532/SK	Data protection 1	Decree proposal of the National Security Agency on the content and extent of operational documentation kept by the certification authority and on the security rules and rules on the execution of certification activities.
35	Slovakia	2008/531/SK	Data protection 1	Decree proposal of the National Security Agency on the conditions for providing accredited certification services and requirements for an audit, the extent of an audit and the qualification of the auditors.
36	Slovakia	2008/530/SK	Data protection 1	Decree proposal of the National Security Agency which stipulates details on requirements for secure devices for the creating of time stamps and requirements on products for electronic signatures (on electronic signature products).
37	Slovakia	2008/529/SK	Data protection 1	Decree proposal of the National Security Agency on the format, content and administration of certificates and qualified certificates and on the format, periodicity and method of issuing an index of cancelled qualified certificates (on certificates and qualified certificates).
38	Slovakia	2008/528/SK	Data protection 1	Decree proposal of the National Security Agency on the format and method of creating advanced electronic signatures, the method of publishing the public key of the agency, the conditions of validity for the advanced electronic signature, procedure during the verification and verification conditions of the advanced electronic signature, format of the time stamp and method of creating it, requirements on the source of time data and requirements for keeping time stamp documentation (on the creation and verification of the electronic signature and time stamp).
39	France	2008/453/F	Data protection 1	Decree No 2008- of 2008 regarding the implementation of Articles 9, 10 and 12 of Order No 2005-1516 of 8

	Country	Reference	Category	Title
				December 2005 on the security of information exchanged by electronic means.
40	Germany	2008/348/D	Data protection 1	Act on Personal Identity Cards and Electronic Identification and amending further regulations (Personal Identity Card Act – PAG).
41	Czech Republic	2008/75/CZ	Data protection 1	Draft Act on electronic transactions, personal identification numbers and authorised document conversion, amending certain Acts relating to the adoption of the Act on electronic transactions, personal identification numbers and authorised document conversion.
[ ]	Italy	2008/48/I	[Unknown]	Draft Ministerial Decree pursuant to Article 8(1) of Decree-Law No 144 of 27 July 2005, converted with amendments by Law No 155 of 31 July 2005 which replaces that issued on 15 August 2005.
42	Hungary	2008/16/HU	Surveillance (vehicles)	The draft GKM. Decree on general requirements for devices capable of imaging vehicles and their licence plates.
43	Denmark	2007/677/DK	Chemicals (weapons, explosives)	Order restricting sales of fertilizer containing ammonium nitrate.
44	Netherlands	2007/617/NL	Data protection 1	Decree on the reliability and confidentiality of electronic case-list message-handling.
45	Germany	2007/604/D	Telecommunications equipment	Technical Guideline outlining the requirements for the implementation of legal measures for monitoring telecommunications [German designation: TR TKÜ], edition 5.1.
46	Denmark	2007/556/DK	Data protection 1	Introduction of mandatory open standards for data exchange between public authorities.
47	Denmark	2007/555/DK	Data protection 1	Introduction of mandatory open standards for document exchange.
48	Denmark	2007/554/DK	Data protection 1	Introduction of mandatory open standards for electronic purchasing in the public sector.
49	Denmark	2007/553/DK	Data protection 1	Introduction of mandatory open standards for digital signatures.
50	Denmark	2007/552/DK	Data protection 1	Introduction of mandatory open standards for public-sector websites/ homepages and accessibility.
51	Denmark	2007/551/DK	Data protection 1	Introduction of mandatory open standards for electronic case and document management.
52	Denmark	2007/550/DK	Data protection 1	Introduction of mandatory open standards for the State in relation to IT security.
53	Germany	2007/462/D	Telecommunications equipment	Article 13 of the Act re-regulating telecommunications monitoring and other covert investigative measures and transposing Directive 2006/24/EC (amendment to the Order on the technical and organisational implementation of measures for monitoring telecommunications [German designation TKÜV]).
54	Italy	2007/449/I	Data protection 1	Draft Interministerial Decree of the Minister for the Interior, the Minister for Reform and Innovation in Public Administration and the Minister for the Economy and Finances, on: ‘Technical and security rules on technology and materials used to manufacture electronic identity cards, electronic identity documents and national services cards, and the methods for use’.
55	Germany	2007/369/D	Data protection 1	Order on the capture and quality assurance of photographs and fingerprints within the passport authorities and the

	Country	Reference	Category	Title
				transmission of passport data to the passport manufacturers (Passport Data Capture and Transfer Order - German designation PassDEÜV).
56	Czech Republic	2007/357/CZ	Chemicals (weapons, explosives)	Draft Act amending Act No. 19/1997 Coll. on certain measures associated with the prohibition of chemical weapons and amending Act No. 50/1976 Coll. on town and country planning and building regulations (the Construction Act), as amended, Act No. 455/1991 Coll. on business activities (the Business Act), as amended, and Act No. 140/1961 Coll., the Penal Act, as amended (hereinafter "the Act").
57	Netherlands	2007/342/NL	Telecommunications (emergency services)	Regulation on preparations for exceptional circumstances for the telecommunications sector 2007.
58	Belgium	2007/292/B	Surveillance (persons)	Draft Royal Decree defining the way in which the presence of surveillance cameras must be indicated.
59	Belgium	2007/286/B	Vehicles (transport of valuables)	Draft Royal Decree amending the Royal Decree of 7 April 2003 regulating certain methods of surveillance and of protection of the transport of valuables and relating to technical specifications of vehicles for transporting valuables.
60	Hungary	2006/567/HU	Weapons	The Decree issued by the Minister for the Economy and Transport on the marking of military technological products and the recording of military technological products and services.
61	Poland	2006/537/PL	Protective clothing	Order of the Chief Commandant of the State Fire Service of 2006 on patterns and detailed requirements, technical and quality specifications of uniform elements, special clothing and personal protection used in the State Fire Service.
62	Germany	2006/453/D	Telecommunications equipment	Technical Guideline outlining the requirements for the implementation of legal measures for monitoring telecommunications [German designation: TR TKÜ], edition 5.0.
63	Sweden	2006/366/S	Chemicals (weapons, explosives)	Order amending the Order (1988:1145) on flammable goods and explosives.
64	Sweden	2006/360/S	Private Security Services	The National Police Board’s administrative provisions and general guidance on the Act (1974:191) and the Order (1989:149) on security companies.
65	Netherlands	2006/347/NL	Telecommunications (emergency services)	The Regulation on the preparation for exceptional circumstances for the telecommunications sector 2006.
66	Belgium	2006/319/B	Private Security Services	Draft Ministerial Decree specifying the way in which the start and end of the surveillance zone referred to in Article 11(3) of the Act of 10 April 1990 regulating private and personal security are to be indicated.
67	Netherlands	2006/283/NL	Police / Fire Service equipment	Decree on technical aids for criminal proceedings.
68	Netherlands	2006/243/NL	Data protection 2	Decree of , amending the Decree on the provision of telecommunications data.
69	Belgium	2006/151/B	Private Security	Draft Royal Decree regulating the model, content, method of carrying and using spray cans and handcuffs by members of

	Country	Reference	Category	Title
			Services	security services for public transport companies.
70	Poland	2006/43/PL	Compliance assessment defence and security articles	National Defence and Security Products Compliance Act.
71	Slovenia	2006/35/SI	Chemicals (weapons, explosives)	Strategic Materials Act.
72	Belgium	2006/28/B	Surveillance (persons)	Draft Royal Decree on the installation and operation of surveillance cameras in football stadiums.
73	Belgium	2006/20/B	Data protection 2	Draft Act amending Article 21(2) of the Act of 11 March 2003 on certain legal aspects of Information Society services, as amended by the Act of 20 July 2005 on various provisions.
74	Slovakia	2006/7/SK	Physical security	National Security Authority Decree, amending National Security Authority Decree No. 336/2004 Coll. on physical security and building security.
75	Slovakia	2005/710/SK	Physical security	Draft National Security Authority Decree of 2005, amending National Security Authority Decree No. 337/2004 Coll., laying down details of the certification of mechanical barrier devices and technical protection devices and their use.
76	Germany	2005/641/D	Data protection 2	Draft Act on the standardisation of regulations on certain electronic information and communications services (Electronic Commerce Standardisation Act - German designation: EIGVG).
77	Austria	2005/620/A	Physical security	Special scheme "Security in residential building" pursuant to Section 7(5) of the Lower Austrian Housing Promotion Act 2005.
78	Austria	2005/514/A	Data protection 1	Draft Order of the Federal Minister for Justice introducing new regulations for electronic legal transactions (Order of the Federal Minister for Justice on electronic legal transactions - ERV 2005).
79	Belgium	2005/480/B	Vehicles (transport of valuables)	Draft Royal Decree amending the Royal Decree of 7 April 2003 regulating certain methods of surveillance and of protection of the transport of valuables and relating to technical specifications of vehicles for transporting valuables.
80	Slovenia	2005/420/SI	Data protection 2	Rules governing equipment and interface units for the lawful interception of communications (8 pages).
81	Belgium	2005/312/B	Weapons	Preliminary draft law regulating economic activities and individuals with weapons.
82	Sweden	2005/264/S	Weapons	The National Police Board's administrative provisions and general guidance on the storage and transport of firearms and ammunition by the police and other national authorities (RPSFS 2005:00, FAP 943-1).
83	Belgium	2005/195/B	Data protection 1	Draft Royal Decree establishing the specifications and registration of reading equipment for the electronic ID card and social ID card.
84	Latvia	2005/132/LV	Private Security	Draft law "Security Guard Activities Law".

	Country	Reference	Category	Title
			Services	
85	Latvia	2005/29/LV	Private Security Services	Draft Law "Security Guard Activities Law".
86	Germany	2004/548/D	Telecommunications equipment	Order on the technical and organisational implementation of measures for monitoring telecommunications.
87	Netherlands	2004/509/NL	Telecommunications equipment	Exemption regulation on divergent use of frequency space by the intelligence and security services.
88	Netherlands	2004/495/NL	Data protection 2	Decree pursuant to Article 28 of the Act on intelligence and security services (Dutch abbreviation WIV 2002).
89	Austria	2004/321/A	Data protection 1	Order amending the Signatures Order.
90	Germany	2004/318/D	Telecommunications equipment	Technical Guideline describing the requirements for the implementation of legal measures for monitoring telecommunications (TR TKÜ), edition 4.1.
91	Netherlands	2004/128/NL	Data protection 2	Decree on requests for telecommunications data.
92	France	2004/25/F	Data protection 1	Order of amending the Order of 31 May 2002 on recognition of the qualification of electronic certification-service-providers and on accreditation of the bodies responsible for the assessment.
93	Portugal	2003/310/P	Data protection 1	Draft Regulatory Decree regulating Decree-Law No 62 of 3 April 2003, amending Decree-Law No 290-D of 2 August 1999, approving the legal system of electronic documents and of digital signatures.
94	Finland	2003/257/FIN	Data protection 1	Government Bill to Parliament for the Data Protection Act in electronic communications and on amending some associated laws.
95	Netherlands	2003/230/NL	Alarm systems	NCP product registration regulations.
96	Italy	2003/219/I	Data protection 1	Draft decree of the President of the Republic concerning regulations on provisions for the use of certified electronic mail (email).
97	Netherlands	2003/184/NL	Data protection 2	Draft Decree regulating the safety measures to be taken by providers of public telecommunications networks or public telecommunications services, such measures pertaining to data on the tapping and recording of telecommunications (Decree on the safeguarding of data with regard to the tapping of telecommunications).
98	France	2003/127/F	Data protection 1	Draft Act for Confidence in the Digital Economy.
99	United Kingdom	2003/109/UK	Data protection 1	Code of Practice on Voluntary Retention of Communications Data under Part 11: Anti Terrorism Crime and Security Act 2001.
100	Belgium	2003/91/B	Vehicles (transport of	Draft Royal Decree regulating certain methods of surveillance and of protection of the transport of valuable goods and

	Country	Reference	Category	Title
			valuables)	relating to technical specifications of vehicles intended to transport valuable goods.
101	United Kingdom	2003/53/UK	Dual-use	Export of Goods, Transfer of Technology And Provision of Technical Assistance (Control) Order.
102	Italy	2003/29/I	Data protection 1	Draft legislative decree transposing Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
103	Finland	2002/365/FIN	Data protection 1	Government Bill to Parliament as a law on amending the Population Data Act and the Identity Card Act.
104	Italy	2002/310/I	Data protection 1	Draft Decree of the Prime Minister laying down technical regulations for the generation, attachment and verification of electronic signatures based on qualified certificates.
105	Spain	2002/301/E	Data protection 1	Preliminary draft Act on electronic signatures.
106	Netherlands	2002/213/NL	Data protection 2	Draft Decree amending the Decree on tapping public telecommunications networks and services, the Decree on the provision of telecommunications information and the Decree on the special gathering of numerical telecommunications data in connection with the establishment of the Act on intelligence and security services 2002.
107	Germany	2002/207/D	Data protection 2	First Order amending the Order on the technical and organisational implementation of measures for monitoring telecommunications.
108	Netherlands	2002/132/NL	Radioactive detection equipment	Draft Decree regulating the detection of radioactive scrap metal (Decree on the detection of radioactive scrap metal).
109	Sweden	2002/82/S	Weapons	Administrative provisions and guidelines of the National Police Board on weapons legislation (Swedish designation: RPSFS 2002:00,FAP 551-3).
110	Netherlands	2002/383/NL	Radioactive detection equipment	Regulation by the Secretary of State for Housing, Planning and the Environment and by the Secretary of State for Social Affairs and Employment regulating the detecting and recording methods for the measuring of the presence of ionised radiation in scrap (Regulation on detection, recording and knowledge requirements for contaminated scrap metal).
111	Germany	2001/480/D	Telecommunications equipment	Order on the technical and organisational implementation of measures for monitoring telecommunications (Order on monitoring telecommunications [German designation: TKÜV]).
112	Belgium	2001/474/B	Data protection 1	Belgian draft on the introduction of an electronic identity card.
113	Finland	2001/469/FIN	Data protection 1	Regulation by the Communication Bureau regarding confidentiality and data security requirements for the operations of certifiers providing qualified certificates to the public.
114	Finland	2001/468/FIN	Data protection 1	Regulation by the Communication Bureau regarding the obligation to notify the Communication Bureau of certifiers providing qualified certificates to the public.

	Country	Reference	Category	Title
115	France	2001/448/F	Data protection 1	Draft Decree on the assessment and certification of the security of information technology products and systems.
116	Belgium	2001/432/B	Vehicles (transport of valuables)	Draft Royal Decree on technical specifications and the type-approval of vehicles intended to transport valuable goods, used by security companies and internal security services.
117	Belgium	2001/281/B	Vehicles (transport of valuables)	Draft Royal Decree regulating specific methods to protect the transport of valuables.
118	Spain	2001/218/E	Data protection 1	Draft Royal Decree implementing Article 81 of Act No 66/1997 of 30 December 1997 on fiscal, administrative and social measures, regarding the provision of security services for the Spanish National Mint - the Royal Mint, in electronic, computer and telematic communications with the public administrations.
119	Finland	2001/125/FIN	Data protection 1	Electronic Signature Act.
120	Spain	2001/109/E	Private security services	Draft Royal Decree amending certain articles of the regulation on private security approved by Royal Decree 2364 of 9 December 1994.
121	Belgium	2001/103/B	Vehicles (transport of valuables)	Draft Royal Decree on technical specifications and type-approval of vehicles intended to transport valuable goods, used by security enterprises and internal security services.

Source: Ecorys based on TRIS database.

Part III - Conformity assessment and certification for security products

7 EU 'generic' framework for conformity assessment and certification of products

7.1 Introduction

This chapter provides a brief overview of the EU regulatory framework for conformity assessment and certification of products as contained within the New Legislative Framework (NLF). This Framework is of relevance to the present study as it describes the approach to be followed – where possible – by the EU and Member States with regard to regulations setting (essential) requirements to be met by products within the Internal Market and corresponding procedures for conformity assessment.

To date, in terms of EU legislation, the use of the NLF has mainly related to aspects such as protection of health and safety of products but also including electromagnetic compatibility. The utilisation of the NLF to cover requirements related to security aspects and performance of products (and services) is, therefore, an issue open to further scrutiny. Nonetheless, in principle at least, the NLF could form the basis for any future regulatory approach used to set inter alia performance requirements for security products and technologies. Moreover, the NLF provides for a range of possible procedures (so-called modules) that should enable conformity assessment to cover not only individual equipment but also security systems (including related services) provided that appropriate performance indicators can be set for the system as a whole. Finally, moving beyond purely technical performance requirements, it may be possible to cover other aspects such as privacy and other ethical dimension; again subject to the definition of appropriate performance indicators against which conformity with regulations may be assessed.

7.2 The New Legislative Framework (NLF)

The New Legislative Framework (NLF) was adopted in European Council on 9 July 2008 and published in the Official Journal on 13 August 2008. The legal texts published on OJEU are:

- Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC;
- Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93;
- Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC.

The objective of the package is to facilitate the functioning of the internal market for goods and to strengthen and modernise the conditions for placing a wide range of industrial products on the EU market. The package builds upon existing systems to introduce clear Community policies which will strengthen the application and enforcement of internal market legislation. *Inter alia*, the NLF:

- Enhances the confidence in and quality of conformity assessments of products through reinforced and clearer rules on the requirements for notification of conformity assessment bodies (testing, certification and inspection laboratories) including the increased use of accreditation; a reinforced system to ensure that these bodies provide the high quality services that manufacturers, consumers and public authorities need;

- Establishes a common legal framework for industrial products in the form of a toolbox of measures for use in future legislation**.** This includes provisions to support market surveillance and application of CE marking, amongst other things and it sets out simple common definitions (of terms which are sometimes used differently) and procedures which will allow future sectoral legislation to become more consistent and easier to implement.

Concerning the last point above, the Decision (768/2008/EC) reflects a commitment by the Commission, Member States and the European Parliament towards a consistent framework for sectoral Community Harmonisation Legislation on products when such legislation is revised or new legislation is adopted. This commitment requires that the provisions within the Directive are to be followed unless the sectors concerned can demonstrate a strong need for departing from them. The Decision includes: harmonised provisions on procedures for conformity assessment; harmonised procedures notifying the EU of the appointment of independent bodies that undertake certain of those conformity assessment procedures ("Notified Bodies"); harmonised provisions on the duties of 'actors' in the product supply chain from manufacturer to distributor; harmonised definitions; and certain rules and conditions for affixing CE marking[93].

7.3 Overview of NLF approach

7.3.1 Essential requirements, technical specifications and harmonised standards

The general approach adopted within the New Legislative Framework (NLF) is for European Commission directives to limit legislative harmonisation to only the "*essential requirements*" of public interest[94] – such as protection of health and safety of products – that must be met when products are placed on the market (i.e. essential requirements are mandatory). The essential requirements should include all that is necessary to achieve the objective of the directive; According to the 'Blue Guide'[95]:

- *"These requirements deal in particular with the protection of health and safety of users (usually consumers and workers) and sometimes cover other fundamental requirements (for example protection of property or the environment). Essential requirements are designed to provide and ensure a high level of protection. They either arise from certain hazards associated with the product (for example physical and mechanical resistance, flammability, chemical, electrical or biological properties, hygiene, radioactivity, accuracy), or refer to the product or its performance (for example provisions regarding materials, design, construction, manufacturing process, instructions drawn up by the manufacturer), or lay down the principal protection objective (for example by means of an illustrative list)";*
- *"Essential requirements define the results to be attained, or the hazards to be dealt with, but do not specify or predict the technical solutions for doing so. This flexibility allows manufacturers to choose the way to meet the requirements. It allows also that, for instance, the materials and product design may be adapted to technological progress";*
- *"Although no detailed manufacturing specifications are included in the essential requirements, the degree of detailed wording differs between directives. The wording is intended to be precise enough to create, on transposition into national legislation, legally binding obligations that can be enforced, and to facilitate the setting up of mandates by the Commission to the European standards organisations in order to produce harmonised standards. They are also formulated as*

---

93 Source: http://www.bis.gov.uk/policies/business-sectors/environmental-and-product-regulations/product-regulation/enforcement-market-surveillance.

94 The essential requirements are to be set out in an annex to a directive.

95 "Guide to the implementation of directives based on the New Approach and the Global Approach", European Commission, (2000). Note: there has been no update of the Blue Book subsequent to the adoption of the NLF in 2008.

to enable the assessment of conformity with those requirements, even in the absence of harmonised standards or in case the manufacturer chooses not to apply them".

Following from the final point above, the underlying principle is for New Approach directives to limit themselves – wherever possible - to expressing essential requirements. As noted above, however, the essential requirements should be sufficiently precise to create legally binding obligations and to assess conformity with them even in the absence of harmonised standards (see below) or where the manufacturer chooses not to apply harmonised standards.

In terms of defining technical requirements, legislation should - where appropriate - have recourse to '*harmonised standards*'; where 'harmonised standards' are defined as standards adopted by one of the European Standards Organisations (ESO)[96]on the basis of a request (mandate) made by the Commission[97]. Accordingly, the NLF foresees that that the ESO are entrusted with the responsibility to draw up harmonised standards corresponding to the technical specifications necessary to meet the essential requirements of a directive. Harmonised standards are not mandatory but there is a presumption that products manufactured in accordance with relevant harmonised standards are conformant to the essential requirements of the directive. It remains open to manufacturers to pursue alternative approaches in order to conform to essential requirements but, in such instances, there is an obligation on manufacturers to prove that products are conformant to essential requirements.

Although the general approach of the NLF is to limit legislative harmonisation to the setting out of essential requirements, this does not completely preclude that detailed technical specifications may be set out in the legislation concerned[98]. The absence of European harmonised standards – or other detailed technical specifications set out on the legislation – does not imply that there are no requirements to be met, as the essential requirements apply to all products (and features and functions thereof) covered by a directive. In such circumstances – and as is also the case if a manufacturer pursues an alternative approach than applying harmonised standards – a manufacturer is required to seek a formal opinion from a notified body (see below) in order to comply with the conformity assessment requirements of a directive[99].

7.3.2 Organisation of conformity assessment system and notification

Notification is an act to inform the Commission and other Member States that a body fulfilling the relevant requirements has been designated to carry out conformity assessment according to a directive(s). Member States are required to notify the Commission and other Member States as to the bodies authorised to carry out third-party conformity assessment tasks under Community Harmonisation Legislation. To this end, Member States are required to designate a *notifying authority* responsible for setting-up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies; Member States may designate a national accreditation body (see below) to be the notifying authority.

---

96 European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardisation (Cenelec) and European Telecommunications Standards Institute (ETSI).

97 Such requests should be made in accordance with the provisions of Directive 98/34/EC (Article 6). After consultation with Member States, the Commission issues a mandate for harmonised standards to be prepared.

98 Decision 768/2008/EC provides that: "where health and safety, the protection of consumers or the environment, other aspects of public interest, or clarity and practicability so require, detailed technical specifications may be set out in the legislation concerned.

99 In such cases, it may be appropriate to reference national or other non-harmonised standards or alternative reference requirements (e.g. industry/professional 'standards').

A *notified body* is a conformity assessment body that has been notified by the (national) notifying authority to the Commission (and other Member States) as meeting the necessary requirements (as set out in Decision No 768/2008/EC) for a body authorised to carry out third-party conformity assessment; subject to no objection by the Commission or other Member States. The necessary requirements relate primarily to the technical competence to carry out conformity assessment procedures and the necessary level of independence, impartiality and integrity. In this regard, accredited in-house conformity assessment bodies cannot be a notified body. However, a body belonging to a business association or professional federation may, on condition that its independence and the absence of any conflict of interest is demonstrated, be designated as a notified body.

It may be noted that Regulation (EC) No 765/2008 provides that each Member State is required to appoint a single *national accreditation body* that is the sole body within the Member State to perform accreditation with authority derived from the State .In turn, where a conformity assessment body requests accreditation, it is required to do so with the national accreditation body of the Member State in which it is established[100]. Accordingly, the system for accreditation of conformity assessment bodies rests on national structures but, at the same time, the Regulation also provides for peer evaluation of national accreditation bodies[101]. National authorities are expected to recognise the equivalence of the services delivered by those accreditation bodies which have successfully undergone peer evaluation and thereby accept the accreditation certificates of those bodies and the attestations issued by the conformity assessment bodies accredited by them.

From the above, the NLF is designed to establish a system of accreditation which ensures the mutual acceptance of the level of competence of conformity-assessment bodies. The competent authorities of the Member States should therefore no longer refuse test reports and certificates issued by an accredited conformity-assessment body on grounds related to the competence of that body. This implies that Member States cannot prohibit the placing on the market of products which have been subject to one of the conformity assessment procedures set up by a directive and which a body notified by another Member State has certified. Member States have an obligation to transpose each conformity assessment procedure established in an NLF directive into their national legislation, hence an equivalence of procedures across countries. And, Member States are bound by a mutual acceptance of the competence of accreditation bodies, conformity assessment bodies and, consequentially, certificates of conformity.

Finally, an *accredited in-house body* may be used to carry out conformity assessment activities for the undertaking of which it forms a part for the purpose of implementing certain procedures[102]. Accreditation is to be undertaken in accordance with Regulation (EC) No 765/2008. An accredited in-house body is required to constitute a separate and distinct part of the undertaking and shall not participate in the design, production, supply, installation, use or maintenance of the products it assesses. There is no requirement for accredited in-house bodies to be notified to the Commission of Member States, but information concerning its accreditation shall be given by the undertaking of which it forms a part or by the national accreditation body to the notifying authority (see above) at the request of that authority.

---

[100] Where that Member State does not have a national accreditation body or such a body does not provide certain accreditation services, then recourse may be made to the national accreditation body of another Member State.

[101] European accreditation infrastructure / European co-operation for Accreditation.

[102] Specifically, Modules A1, A2, C1 or C2, as described in Section 7.3.3.

7.3.3 *Conformity assessment modules*

The NLF provides for a set of common conformity assessment procedures, referred to as 'Modules'. In determining which procedure(s) are relevant for a particular product, the following criteria should be applied:

- Appropriateness to the type of product;
- Nature and level of the risk involved;
- Mandatory involvement of third party:
  - Where involvement of a third party conformity assessment body is mandatory, the need for the manufacturers to have a choice between implementation of a quality assurance system or product certification.
- Conformity assessment should be proportionate and effective (i.e. to avoid imposing modules which are too burdensome in relation to the risks covered by the legislation concerned):
  - Account should be taken of the economic infrastructure of the sector (e.g. type and size of companies, complexity of product technology; existence or non-existence of third parties);
  - Account should be takes of the type and importance of production.

The conformity assessment procedures are divided into eight basic modules (A to H), ranging from a manufacturer's declaration through to full quality assurance. In addition, a number of variants based on the basic modules are available. The basic modules and their variants can be combined with each other in order to establish complete conformity assessment procedures. An overview of the modules is shown in Figure 7.1 . The individual modules may cover the product design phase, the production phase, or both. In general, products will be subject to a conformity assessment module in both the design and production phase. Briefly:

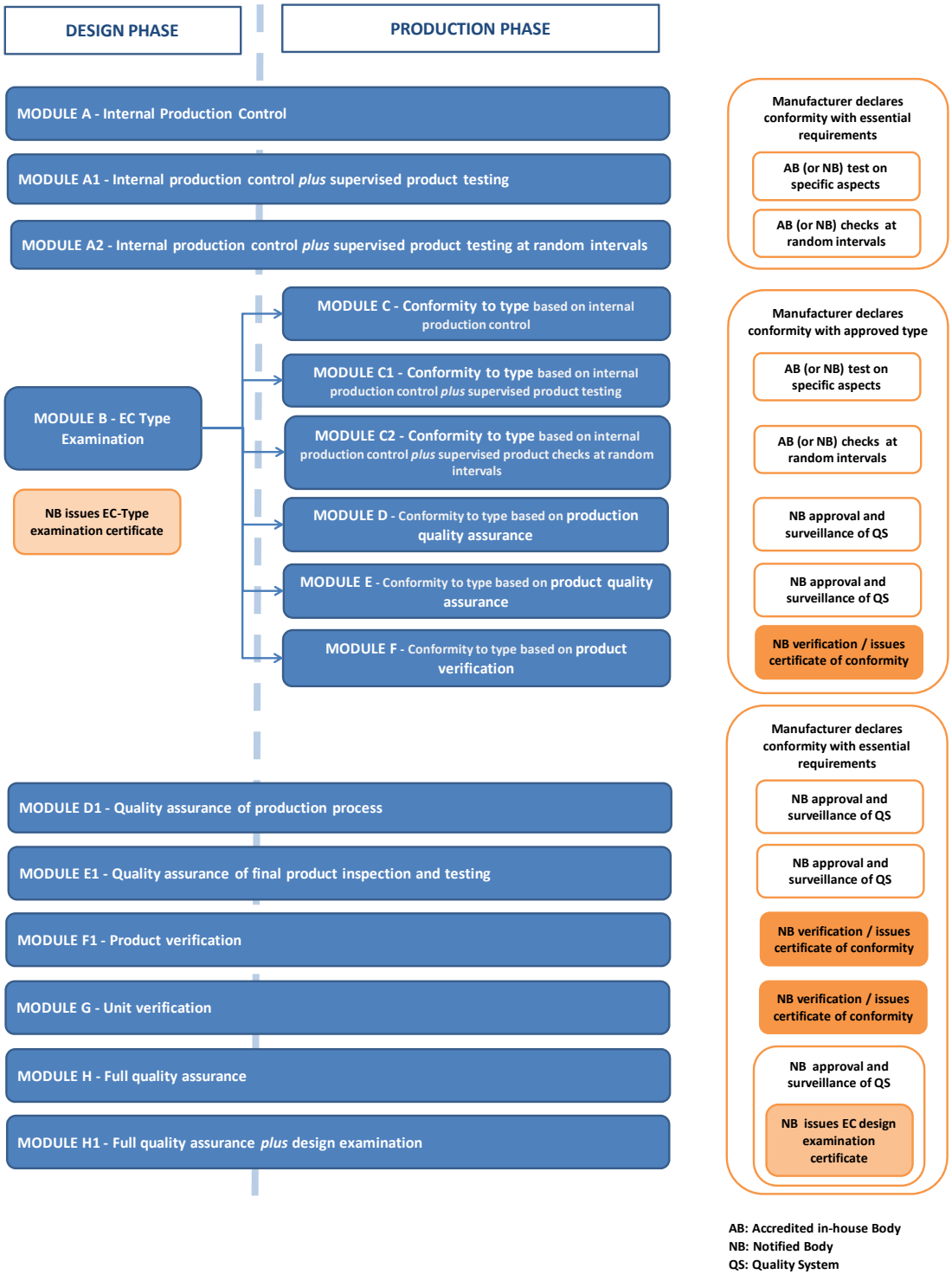
- **Module A** is the least stringent procedure since it provides for conformity assessment to be undertaken without reference to any independent third-party or even an accredited 'in-house' conformity assessment body; i.e. *self-declaration*. The two variants (Modules A1 and A2), provide for a suppliers declaration of conformity with essential requirements to be supported by product testing (either for specific aspects of the product (A1) or on random samples (A2)), which may be undertaken by an accredited in-house body or by a third-party (notified) body;
- **Module B** provides for a notified body to undertake an *examination of the technical design of a product* to verify that the technical design of the product meets the requirements of the legislative instruments that apply to it. On the basis of an examination (and tests) of the technical documentation and specimen supplied by the manufacturer, the notified body issues an EC-type examination certificate (for those product designs/specimens meeting the relevant legislative requirements). Modules applied subsequent to a Module B procedure, are based on providing conformity assessment in relation to the type (of product) described in the EC-type examination certificate (i.e. support for manufacturer's declaration of conformity to type);
- **Module C** (and variants thereof) are analogous to Module A (and variants thereof), but with the product design having in the first instance been subject to an examination of the technical design of a product (i.e. Module B). As with the variants of Module A, the variants C1 and C2 allow for conformity assessment to be undertaken by an accredited in-house body (or by a third-party (notified) body);
- **Module D, Module E** and **Module H**(and their variants) provide for conformity assessment to be based upon the operation of an *approved quality control systems*[103].These provide an alternative to product examination/testing by third-party body but do require that the operated quality control system is approved by a notified body and subject to surveillance by the same. As noted above, under the NLF, if involvement of a third party conformity assessment body is

[103] They differ in terms of the comprehensiveness of the examinations and tests within the quality system: Module E applies for examinations and tests after manufacture; Module D applies to examinations and tests before, during and after manufacture; and Module H extends also to the design phase.

mandatory then manufacturers must be given a choice between implementation of a quality assurance system or product certification (see next bullet);

- **Module F** and **Module G** (and the variant F1) provide for independent third-party conformity assessment (i.e. by a notified body) leading to the issuing of a *certificate of conformity*. Module F provides for examination/testing of products produced in series (either for every product or random samples) to provide assurance that each product is in compliance, while Module G provides for examination/testing of individual units to provide assurance that a single item is in compliance.

Figure 7.1 Overview of conformity assessment modules



8 Supra-national approaches to conformity assessment and certification in the security domain

8.1 Introduction

Following from the previous chapter which outlined the general EU framework for conformity assessment to be applied for sectoral harmonisation legislation for products in the internal market, this chapter provides an overview of some supra-national approaches to conformity assessment and certification in specific security domains.

It is important at the outset to note that in most instances, the approaches outlined in this chapter are in many cases relatively new and, accordingly, their lack of maturity makes it difficult to assess their relative strengths or weaknesses. Moreover, it should be noted that the examples provided in this chapter are illustrative and do not attempt to provide an exhaustive description of relevant conformity assessment and certification schemes. Equally, this chapter makes no attempt to cover national schemes, or those restricted to only a few countries. In fact, it is the very multitude of national approaches that lies behind the efforts to develop common approaches to CAC described in this chapter.

As a further comment, it should be noted that a number of EU supported projects (completed and on-going) have addressed the issue conformity assessment and certification in the area of security. We may note, for example, BioTesting Europe[104], Staborsec (Standards for Border Security Enhancement)[105], Creatif (Network for Testing Facilities for CBRNE detection equipment)[106].

8.2 Screening equipment in the aviation sector: ECAC-CEP

Not least as a consequence of the terrorist attacks within the sector, aviation is a sector that has clearly been a focus of attention for public authorities. This has resulted in the establishment of a regulatory framework for aviation and airport security that overlays provisions at international, European and national levels. With regard to security equipment, the EU regulatory framework identifies acceptable screening methods for passengers and luggage. The regulations also establish technical specifications for minimum performance criteria for several categories of equipment (metal detectors, x-ray equipment, EDS. EDTS).

Alongside the performance criteria established under EU regulations, the European Civil Aviation Conference (ECAC) has established a Technical Task Force that undertakes the development of technical specifications and testing methodologies to verify compliance with the standards required for deployment in European Airports. Further, ECAC has established a process for evaluating security equipment: the Common Evaluation Process for security equipment (CEP). This framework incorporates unified testing methodologies (Common Testing Methodologies, CTM) per type of

---

104 http://www.biotestingeurope.eu/ This project aimed to set out the prerequisites for the establishment of testing and certification capabilities on biometric components and systems in Europe.

105 http://sta.jrc.ec.europa.eu/index.php/prima-action/60-staborsec Deliverable D5.1 contains a list of existing certification procedures for border security standards.

106 http://www.creatif-network.eu/home.html.

equipment. To date, CTMs have been established for imaging X-ray equipment, explosive detection systems (EDS), liquid explosive detection systems (LEDS) and security scanners (SS), whereas CTMs for Walk Through Metal Detectors (WTMD) and Explosive Trace Detectors (ETD) are in preparation.

If a new type of equipment/technology is introduced that is not on the EU approved list of screening methods for passengers and luggage, a pilot evaluation is performed. Permission for a pilot is only granted by the EU if the equipment is safe and if the existing level of security is not reduced. Demonstration of these prerequisite conditions is established through tests undertaken in laboratories such as the ECAC approved test centres (see below). During the pilot evaluation it has to be constantly verified that these safety and security conditions are still met. If the pilot is successful then both appropriate EU regulations – designating the equipment/technology as an acceptable screening method – and a CTM have to be developed. Before the CTM can come into force, there is also a pilot to investigate whether the CTM is feasible and robust. To date, the main parties investing in developing CTMs are the United Kingdom, the Netherlands, France and Germany.

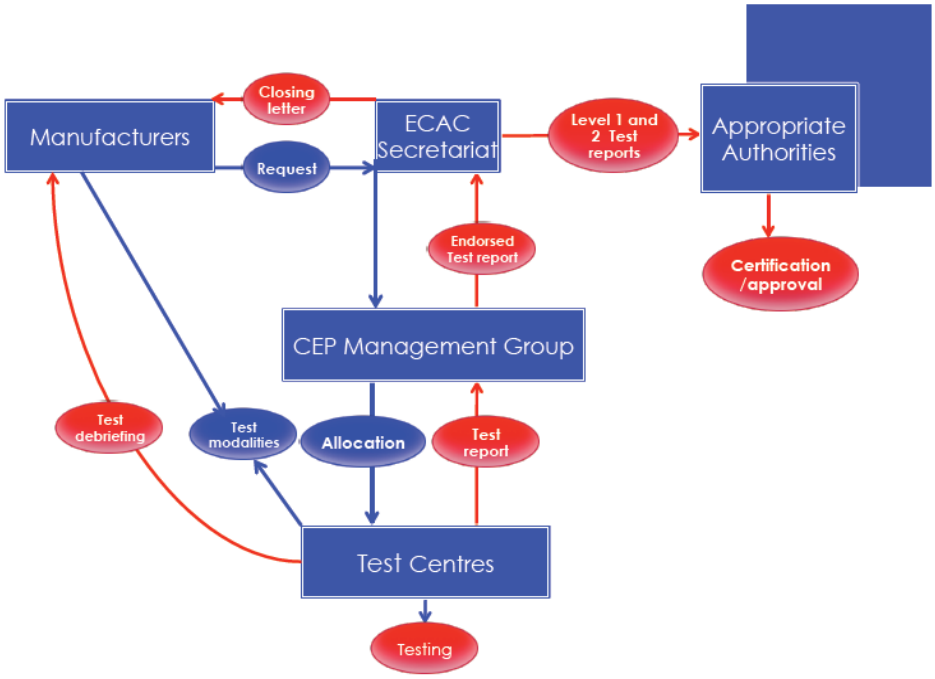
Alongside technical aspects, the CEP also sets out administrative procedures with the goal of supplying the service to ECAC member states of delivering a robust, reliable, repeatable and broadly acceptable basis for national certification. Actual testing is done by a limited number of highly specialised laboratories, which have been designated to the CEP by their national Appropriate Authorities. Currently there are 4 test centres where EDS can be assessed and 3 test centres where LEDS can be assessed. In the CEP the functionality of a system is evaluated, not the specific technical design. As an indication of the quantity of tests performed under the supervision of the ECAC, in the 2010-2011 timeframe, 28 tests on security equipment of manufacturers are reported[107].

Manufacturers can enrol their system for conformity assessment at ECAC. ECAC plans the assessments and notifies the manufacturers where and when their equipment can be tested. The EDS or LEDS passes or fails against the appropriate standard as laid down in the European legislation; the result (standardised test report) is transmitted to the manufacturer and the ECAC Member States that are signatories to the CEP Administrative Arrangements. The manufacturer also receives verbal feedback within specified boundaries. If the system is attributed a standard, this is passed on to the appropriate authorities of the ECAC member states, which can certificate the equipment based on the test results and subsequent attributed Standard. Usually Member States convert a ‘pass’ directly into a certification, sometimes an exception is necessary though in case of more stringent national regulations. Under the CEP there is, however, no provision for the formal approval or certification of equipment as complying with EC requirements, although the ECAC requirements as laid down in ECAC Doc.30 are identical to the EC requirements. Such approval and certification, as with other security equipment not covered by CEP, remains the responsibility of the appropriate authority in each ECAC Member State.

While it is evidently the aim of the CEP to provide a harmonised evaluation of different categories of security equipment, it is only applied to a limited number or categories of equipment (and technologies) and does not provides for a common EU/European-wide certification programme or for direct enforced mutual recognition of equipment certified at a national level, neither does it provide for conformity assessment (or certification) beyond the aviation sector.

[107] Source: https://www.ecac-ceac.org; information as of August 2011.

Figure 8.1 Overview of ECAC Common Evaluation Process



8.3 Security alarm systems: CertAlarm

CertAlarm[108] represents one recent industry led initiative (its first certificates were issued in May 2010) to provide a European-wide scheme for certification of 'traditional' security products. CertAlarm is focussed on fire protection and detection systems and security systems; the latter currently covering intrusion and hold-up alarm systems, which are to be extended to other equipment such as CCTV systems, access control systems etc.).

The CertAlarm Certification Schemes provide a proof of conformity the European (EU) product, system, installation and service standards. The scheme is based on the principle of independent third-party assessment and certification of security products. In February 2011, the European cooperation for Accreditation (EA)[109] confirmed the status of CertAlarm as a scheme covered by the EA Multilateral Agreement (MLA).

To a large extent the development of CertAlarm can been seen as a reaction to the slow embrace by certifying bodies across Europe of a common approach, and to industry's desire to have an EU-wide solution for certification of their security products. Some stakeholders, notably certifying bodies, reject the need for a new scheme and point to the fact that existing certification arrangements could be used if appropriate EU standards were established and adopted for a wider range of security sectors/products. Specifically, they argue that the lack of a single EU-wide certification approach is due to the lack of market acceptance and use of European standards, which means that certifying bodies continue to certify mainly on the basis of national standards as these continue to be used by most architects, construction companies, and industrial clients and in procurement contracts (including public procurement contracts). In other words, they argue that the

[108] http://www.certalarm.org/ca/index.php.

[109] http://www.european-accreditation.org/content/home/home.htm. The EA is the official European (EU) accreditation infrastructure, in accordance with the adoption of Regulation EC 765/2008 adopted as part of the New Legislative Framework (see Section 7.2).

lack of an EU common approach is a reflection of deficiencies in EU standards and not in conformity assessment systems. Accordingly, if appropriate EU standards existed then all certifying bodies would certify on the basis of such standards, therefor removing problem with the acceptance and mutual recognition of different certificates.

Notwithstanding the above comments, some stakeholders point to the certification scheme and CertAlarm label as a model that could be extended to other security products, though it seems too early to predict if CertAlarm will gain wide market recognition. To date, only a handful of partners have agreed to follow the scheme and to award the CertAlarm certificate.[110] Attempts to involve the certifying bodies and the insurance industry have so far yielded few results. Further, only 9 certificates have so far been issued for products from 4 companies. In view of the infancy of the scheme and the limited number of products that have undergone evaluation, it is too early to assess how the CertAlarm schemes may develop or evaluate its performance.

8.4 Security of IT products: Common Criteria

The Common Criteria (CC) – full title, Common Criteria for Information Technology Security Evaluation) – is an ISO standard (ISO15408). Together with the Common Methodology for Information Technology Security Evaluation (CEM), the CC provides a framework for the specifying and evaluating the security attributed of IT products. They provide the technical basis for an international agreement – the Common Criteria Recognition Agreement (CCRA) – providing for mutual recognition of certification of secure IT products. A brief overview, paraphrased from the introduction to the CC, is given in the following box.

Summary of the introduction to the Common Criteria[111]

1. The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software;
2. The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs;
3. The CC is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality;
4. The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products;
5. Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used;
6. The CC addresses protection of assets from unauthorised disclosure (confidentiality), modification (integrity), or loss of use (availability). The CC may also be applicable to aspects of IT security outside of these three. The CC is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities;

[110] The CertAlarm website lists only two contracted certification bodies (ANPI of Belgium and Telefication of the Netherlands) and 3 recognised test laboratories, these being the aforementioned certification bodies plus Kriwan Testzentrum GmbH from Germany.

[111] "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model", July 2009, Version 3.1 Revision 3 Final. Available at: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf.

7. Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below:
   a. The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality;
   b. The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered;
   c. The CC does not address the evaluation methodology under which the criteria should be applied. This methodology is given in the CEM;
   d. The CC does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework;
   e. The procedures for use of evaluation results in accreditation are outside the scope of the CC. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects;
   f. The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

The Common Criteria are the outcome of the efforts of number of governments (USA, Canada, UK, France, Germany and the Netherlands) to develop harmonised security criteria for IT products. Currently, within the CCRA, there are 15 'Certificate Authorising Member' countries (Australia, New Zealand, Canada, France, Germany, Italy, Japan, Rep. of Korea, Netherlands, Norway, Spain, Sweden, Turkey, United Kingdom, United States) and 11'Certificate Consuming Member' that recognise Common Criteria certificates but do not issues them (Austria, Czech Republic, Denmark, Finland, Greece, Hungary, India, Israel, Malaysia, Pakistan, Singapore). The CCRA – and SOG-IS MRA (see below) – removes the need for duplicate evaluations of IT products and production profiles, saving both vendors and users time and resources.

The Common Criteria offer a framework that enables, on the one hand, users of IT products to specify their security requirements and, on the other, for vendors of IT products to develop/implement IT products, the security attributes of which can be evaluated (by independent testing laboratories). Thus, the Common Criteria provide assurance that the process of specification, of implementation and evaluation of an IT security product has been conducted in a rigorous and standard manner[112]. The underlying strength of the Common Criteria is that it provides for security assurance to be defined using internationally accepted terms and standards. For users, it enables easy comparison of products in terms of the security functionalities that have been tested and the level to which such testing has been performed. For developers/vendors it enables them to demonstrate to an international market that their product has gained an objective (independent) confirmation of the validity of its security claims.

The Common Criteria provide for 7 Evaluation Assurance Levels (EAL) with EAL-1 being the most basic, and EAL7 the most stringent (see Table 8.1); it should be noted that the EAL relates to the extensiveness of the evaluation of a product and not to the 'level' of security provided by a product.

[112] Ernst D. and S. Martin (2010), "The Common criteria Information Technology Security Evaluation – Implications for China's Policy on Information Security Standards", East=West Centre Working Paper, No 108, January 2010.

The CCRA provides for recognition of CC Certificates up to EAL4. Within Europe, recognition of CC certificates up to EAL7 (for IT products related to certain technical domains only)[113] has additionally been agreed under the SOG-IS Mutual Recognition Agreement (MRA)[114] by Finland, France, Germany, the Netherlands, Norway, Spain, Sweden and the UK.

Table 8.1 Common Criteria Evaluation Assurance Levels (EALs)

EAL level	Description
1	Functionally Tested. Provides analysis of the security functions, using a functional and interface specification of the TOE, to understand the security behaviour. The analysis is supported by independent testing of the security functions.
2	Structurally Tested. Analysis of the security functions using a functional and interface specification and the high level design of the subsystems of the TOE. Independent testing of the security functions, evidence of developer "black box" testing, and evidence of a development search for obvious vulnerabilities.
3	Methodically Tested and Checked. The analysis is supported by "grey box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required.
4	Methodically Designed, Tested and Reviewed. Analysis is supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.
5	Semi-formally Designed and Tested. Analysis includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Covert channel analysis and modular design are also required.
6	Semi-formally Verified Design and Tested. Analysis is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.
7	Formally Verified Design and Tested. The formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.

Source: CESG: http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/cc_levels.shtml.

The testing of products is mainly undertaken by independent testing laboratories, with final evaluation of test findings and the issuing of certificates undertaken by the national (government) agencies that are signatories to the CCRA (or SOGIS-MRA). In this respect, testing of products is a commercial activity and costs to developers/vendors can be substantial. In turn, a developers/vendors decision to submit a product for evaluation/certification is a commercial decision, to be set against the market benefits of being able to supply a certified product. In this

[113] For the moment, only the "smart cards and similar devices" technical domain is concerned by this agreement for the high level of recognition. The technical domain "Point of Interaction" is under creation. Source: http://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements.html.

[114] Senior Officials Group Information Systems Security (SOG-IS) of the European Commission. The latest (2010) SOG-IS Mutual Recognition Agreement (MRA) is available at: http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/formal-docs/mra.pdf.

regard, a CC evaluation is often mandatory for IT products procured by governments and, due to its widespread recognition, by main other users.

The use of independent (non-government) testing laboratories and the emphasis on the commercial nature of evaluation and certification can be seen as a shift towards a more private sector orientation, compared to earlier approaches[115]. In turn, this is seen as providing an incentive for the private sector to make the certification scheme successful. The Common Criteria is supposed to engage members of many communities, including developers/vendors and users, based on a consensual approach and dialogue between governments and industry. Nonetheless, the system as a whole is seen by some to still be too bureaucratic (and costly); not least due to the involvement of government agencies (and other closely related bodies) in the determination of standards applied through the Common Criteria.

Despite the good intentions underlying the Common Criteria, a recent paper from the US NSC/CSS[116] Commercial Solutions Centre (NCSC) notes that*: "In theory, countries that recognize Common Criteria evaluations should have considerable clout for convincing vendors to make security improvements to products. In practice, these countries have not cooperated sufficiently to agree upon requirements and many participants do not require the evaluations. The current trend is for countries to create their own testing regimens. In some cases, these competing evaluation schemes will be used to protect indigenous industries, and, more disconcertingly, as an opportunity to force vendors to disclose sensitive information."*[117]

Among the criticisms of CC approach, the following may be noted[118]:

- The CC are generic and do not directly prescribe the security requirements or features expected for a specific class of products;
- The flexible approach permits developers/vendors to limit the scope of evaluation used to obtain certification to certain features of the product and/or to make certain assumptions about the operating environment and the nature and strength of threats to be addressed;
- The CC evaluation methodologies are not tailored to specific technology areas; he CEM is a general set of evaluation activities that make no reference to a specific technology Arguable, although efforts have been made to instil greater confidence by updating and modifying the criteria themselves, it needs to be acknowledged that "*no single set of criteria can be used to produce comparable and effective evaluations for a wide range of technologies*";[119]
- CC evaluations are undertaken at the product or individual system level – referred to as the target of evaluation (TOE) – on the assumption that other systems which the product interacts with are assumed to be under the same security management control and operate under the same security constraints. There are no security requirements that address the need to trust external systems or the communication links to such systems;
- The CC approach takes a product based approach. It covers the design and development phase of IT products (and systems) but not the operational phase. In general the CC currently

---

115 There have been some claims of developers/vendors 'shopping' for laboratories to find those more likely to provide a positive evaluation, though this may equally be a reflection of different fees charged by testing laboratories or the speed of evaluation services.

116 National Security Agency / Central Security Service.

117 NCSA (2011), "Common Criteria Reforms: Better Security Products through Increased Cooperation with Industry", available at: http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf.

118 See, for example, NCSA (2011) ibid footnote 117; Zhou C. and S. Ramacciotti (2011) "Common Criteria: Its limitations and advice on improvement", ISSA Journal, April 2011; information from various blog sources, e.g.: http://blogs.oracle.com/security/entry/the_evolution_of_common_criter ; http://www.ratliff.net/blog/category/common-criteria/ ; http://gcn.com/articles/2007/08/10/under-attack.aspx.

119 Ibid. footnote 117.

focuses on design features and their implementation, but is weaker at addressing potential flaws in development, deployment and life-cycle aspects;
- The CC evaluation process for lower assurance levels (EAL1 to EAL4), which correspond to the levels at which most products are evaluated, are essentially a paper evaluation of the development process and product documentation, not requiring evaluation of software;
- Commonly used protection profiles often do not correspond to the functionality requirements actually required by users.

8.5 Privacy for IT products: EuroPriSe

EuroPriSe, the European Privacy Seal, is a European scheme providing privacy and data protection certification for IT products and IT-based services. The European Privacy Seal embodies a visible trust mark certifying that a product or service has been checked by independent experts and approved by an impartial privacy organisation. EuroPrise started in June 2007 as a pilot project funded by the European Commission's eTEN program120. The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the EU Member States.

Evaluations are undertaken by independent experts, with an expert admission procedure the aims to ensure that private evaluators are independent and reliable and have the necessary qualifications. The EuroPriSe website[121] lists nearly 120 experts but these are predominantly from either Germany or Spain[122], which are hosts to the two organisations (certification bodies) that issue certificates under the scheme. These organisations are the Independent Centre for Privacy Protection (*Unabhängiges Landeszentrum für Datenschutz*, ULD or ICPP), which is the data protection authority of the state of Schleswig-Holstein, Germany and the Madrid and the *Agencia de Protección de Datos de la Communidad de Madrid*, (APDCM) which is the data protection agency for Madrid. The EuroPriSe website indicates that 19 certificates (awarded seals)[123] have been issued.

The criteria used in the evaluations can divided into four different sets. The first set includes fundamental aspects of processing and technical construction. The second test focuses on the legitimacy of data processing, including its legal basis, special requirements to the various phases of the processing, compliance with general data protection principles and duties, special types of processing operations and a number of formalities. The third set considers the technical-organisational measures that support the protection of the data subject, concerning general duties as well as technology and service-specific requirements. Finally, the fourth set ensures that the

---

120 The EuroPriSe consortium was led by the Independent Centre for Privacy Protection (Unabhängiges Landeszentrum für Datenschutz, ULD or ICPP), the data protection authority of the state of Schleswig-Holstein, Germany. The partners from eight European countries included the data protection authorities in Madrid (Agencia de Protección de Datos de la Communidad de Madrid, APDCM) and France (Commission Nationale de L'Informatique et des Libertés, CNIL), the Institute for Technology Assessment of the Austrian Academy of Sciences, London Metropolitan University (UK), Borking Consultancy (the Netherlands), Ernst & Young AB (Sweden), TÜV Informationstechnik GmbH (Germany) and VaF s.r.o. (Slovakia).

121 https://www.european-privacy-seal.eu/.

122 The national breakdown of experts listed on the website is as follows: Argentina (1); Austria (13), Belgium (0), Croatia (2), Finland (3), France (4), Germany (53), Ireland (1), Netherlands (3), Slovak Republic (1), Spain (28), Sweden (3), Taiwan (1), United Kingdom (4), USA (1). Website viewed on 1 July 2011.

123 Website viewed on 1 July 2011. 2 products appear to have been recertified as there is a total list of 21 awarded seals. The geographical breakdown of manufacturers/providers is as follows: Germany (6), Spain (4), Austria (2), Netherlands (2), Belgium (1), Ireland (1), Sweden (1), USA (1).

data subjects' rights are fully respected, in line with the data protection Directive 95/46/EC and the data protection Directive 2002/58/EC in the electronic communications sector. [124]

In view of the limited number of products that have undergone evaluation under the EuroPriSe scheme and the relative infancy of the scheme it is difficult to evaluate its performance. However, it appears that there is relatively limited visibility for the scheme and currently recognition is limited. In this respect, it risks becoming yet another 'certification' scheme alongside national and other schemes trying to provide some form of assessment of the privacy and data-protection characteristics of IT products and services.

8.6 Video surveillance (IP systems): ONVIF and PSIA

While it appear evident, given the nature of security risks, that third-party certification by suitably qualified conformity assessment bodies is necessary it is also possible to point to other private/industry frameworks for security products. As an example, in the area of video surveillance, the Open Network Video Interface Forum (ONVIF)[125] and the Physical Security Interoperability Alliance (PSIA)[126] are two recently created organisations[127] with the aim of developing interoperability standards for Internet Protocol (IP) based security systems[128]. Both these bodies are promoting conformity schemes based on manufacturers undertaking their own conformance testing.

8.7 Video-surveillance in urban areas: Charter for the democratic use of video surveillance ('code of practice')

The 'Charter for a democratic use of video-surveillance'[129] comes out of a project of the European Forum for Urban Security(EFUS)[130] entitled "Citizens, Cities and Video Surveillance"[131], which was supported by the European Commission and involved the participation of 10 members of the EFUS network: Le Havre (France), Saint-Herblain (France), Liège (Belgium), Veneto (Italy), Emilia Romagna (Italy), Sussex Police (United Kingdom), Ibiza (Spain), Rotterdam (Netherlands), Genoa (Italy), and the London Metropolitan Police Service (United Kingdom). The project aimed to develop recommendation for using CCTV in a transparent manner, respecting individuals' rights. These recommendations were incorporated in the Charter, which essentially provides a 'code of practice' providing the basis for the good use of video surveillance in European cities. The Charter was formally presented in Rotterdam on May 28th 2010, with the city of Rotterdam and the city of Saint-Herblain being the first to sign it.

The development of the Charter reflected a common necessity to include in the development and functioning of video-surveillance guarantees that protect citizens' privacy and fundamental liberties; as enshrined in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Charter covers the design, operation and subsequent development of

---

124 For further information, see: EuroPrise Criteria, May 2011, 'https://www.european-privacy-seal.eu/criteria/EuroPriSe%20Criteria%20May%202011%20final.pdf'.

125 http://www.onvif.org.

126 http://www.psialliance.org.

127 Both bodies were created in 2008.

128 Essentially these are video surveillance systems that are able to send and receive data via computer networks and internet.

129 http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_EN.pdf.

130 http://www.efus.eu/en/.

131 http://cctvcharter.eu/index.php?id=31559&L=xrlqcvrrw.

public-surveillance systems (i.e. those operated by public authorities, be they national, regional or local). However, the Charter may (should) be applied to private video-surveillance systems, especially when their use and data might be made available to public authorities. The Charter is based on seven fundamental principles:

- The design and development of video-surveillance systems can only be undertaken in compliance with existing laws and regulations;
- The installation of a video-surveillance system must be justified;
- The design, installation, operation and subsequent development of video-surveillance systems must respect a sound and suitable measure;
- Every authority employing a video-surveillance system must have a clear and coherent policy regarding the operation of their system;
- The right to surveillance of public areas is reserved to carefully limited authorities. These authorities are responsible for the systems installed in their name;
- Check and measure should be put in place to maintain the correct functioning of the video-surveillance systems through a process of independent oversight;
- All must be done to encourage citizen involvement at every stage in the video-surveillance system's life.

In pursuit of the above fundamental principles, the Charter puts forward four 'methodological tools':

- **The undertaking of prior audits to define objectively local needs.** These audits should also allow an evaluation of the feasibility of a video-surveillance project in a given area. Ideally, this audit should be carried out by an external body;
- **Periodical evaluations** serving as an aid to decision making and allowing for a strengthening or repositioning of the video-surveillance system;
- **Training of operators.** The operators are the key-stone of the video-surveillance system. On them largely depends the sound functioning of the system. Their training should include the fundamental principles of this charter but equally the recommendations to be put into practice. The objectives of the system should also form a part of their training. Training ensures quality;
- **A controlling authority** should guarantee adherence to the Charter's principles. The creation of such a local structure could be set in motion either by national law or as a result of local initiative. This authority must be of the greatest possible independence.

On the issue of conformity assessment and certification, under the heading of 'future plans' the Charter includes the provision that cities having signed the charter "*wish for a European label and certification to be put in place*".

9 Overview of US framework for conformity assessment and certification of security products

9.1 Introduction

This Chapter provides a quick scan of the regulatory and conformity assessment framework in the USA. The quick scan focuses on the framework of standardisation and conformity assessment.

9.2 The general context of homeland security

9.2.1 Key elements of national security policy

The aftermath of the 9/11 attacks in September 2001 as well as other terrorist threats, the 'war on terror' (Afghanistan, Irak) and also the 'war on drugs' (Colombia, Mexico) triggered a very strong political attention for security, especially the security of US citizens ('homeland security'). In October 2001 for example the USA Patriot Act[132] was launched, a bill which focused on changes in the law that allowed law enforcement greater surveillance capabilities, enhanced punishments for crimes related to terrorism, and for improving relationships and communication between federal and local law enforcement.[133] Besides that, a dedicated department for national security was institutionalised in 2002 by the Homeland Security Act.[134]

> **The Department of Homeland Security** (DHS) is charged with coordinating activities and improving information sharing efforts among federal, state, local, and tribal government agencies and the private sector.[135] More specific the DHS has multiple 'missions', i.c. (i) preventing terrorism and enhancing US security (this includes aviation security, chemical security, law enforcement, protecting infrastructure, etc.), (ii) securing and managing the US borders (including customs, export/import container security, small vessel security, coast guard, IPR, fraud, etc.), (iii) enforcing and administering US immigration laws (including legal/illegal immigration, human smuggling, etc.), (iv) safeguarding and securing cyberspace (critical infrastructure, classified information, computer crime, etc.) and (v) ensuring resilience to disasters (preparing individual families/persons, disaster response, disaster recovery, communication, etc.).[136]
>
> In 2010 the enacted budget was approximately € 41.7 billion ($ 55,3 billion), while for example the 2004 budget was approximately € 29.1 billion ($ 36.2 billion).[137]

Also in recent years there were several security threats that resulted in (political) attention for homeland security (e.g. an attempted attack in an airplane in 2009, cyber-attacks and hurricane

---

132 USA Patriot Act of 2001, public law 107-56.

133 Oliver, W.M., 'Policing for Homeland Security: Policy & Research', in: Criminal Justice Policy Review, 2009 (20), p. 254.

134 The Homeland Security Act of 2002, public law 107-296.

135 DHS, 'DHS's role in state and local fusion centres is evolving', December 2008.

136 DHS, 'Fiscal Year 2011 – Budget in Brief', 2010 (undated). The exact DHS mission is given in the Homeland Security Act of 2002, public law 107-296, sec. 101 (b). Every policy field has its own policy initiatives and programmes and as a result the regulatory framework is very broad and very diverse. This framework ranges from cargo screening and biometrical identification to launching a critical information website (in case of emergencies) and certification of disaster preparedness programmes. An overview of the main policy fields in 2010 can be found here: http://www.dhs.gov/xlibrary/assets/department-accomplishments-and-reforms-2010.pdf.

137 DHS, http://www.dhs.gov/xabout/budget/ ; Eurostat exchange rates (2004: €1 is $1.2439; 2010: €1 is 1.3257).

Katrina).[138] Since 2002 the National Strategy for Homeland Security is updated on a regular basis. In the 2010 Strategy for Homeland Security one of the main objectives is to strengthen 'security and resilience at home', for example by encountering radicalisation, enhanced emergency capabilities and more public-private partnerships.[139]

The DHS is dealing at the moment with the creation of 'fusion centres'. In 2004 the '9/11 Commission'[140] concluded in her evaluation that a lack of information sharing was one of the problems which hindered the prevention of the attacks. This commission also stressed the importance of sharing of local and state information. Therefore it was decided in 2004 that there should be established a 'Information Sharing Environment'.[141] Since 2006 the Office of Intelligence and Analysis (OIG, office within the DHS) is the executive agency responsible for the 'Fusion Center Initiative' which should create 'a web of interconnected information nodes across the country'.[142]

9.2.2 *Economic priorities related to security*

Despite the fact that in the US policy environment the focus lies on countering specific security threats, they also stress that economic growth and maintaining their economic and technological leadership in the world play an important role for the security of the US. Science and innovation should be top priorities in order to support the US prosperity, defence and international technological leadership.[143] Besides attention for education, investments in R&D, investments in new technologies, etc., this also includes major (federal) spending in defence and security, which is a very strong driver for research and innovation in high-tech security solutions. Ecorys already indicated that the US federal government was responsible for 60% of the total public and private spending on security equipment (which was in 2008 approximately € 42 billion)[144].

There is also a strong economic aspect to the US SAFETY Act, which specifically encourages the development of new and innovative anti-terrorism products and services by providing liability protections for companies that develop products and services used in combating terrorism.[145] Part of this liability protection is a designation and certification procedure, which results *de facto* in a 'seal of approval'. This specific procedure is described in Section 9.5, which follows a description of the general US standardisation and conformity assessment framework.

---

138 DHS, 'Quadrennial Homeland Security Review', February 2010.

139 President of the United States, 'National Strategy for Homeland Security', May 2010.

140 The National Commission on Terrorist Attacks upon the United States.

141 DHS, 'DHS's role in state and local fusion centres is evolving', December 2008. The 'Intelligence Reform and Terrorism Prevention Act' of 2004 is one of the main drivers for this process, besides the 'Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment' Office of the Press Secretary, December 16, 2005.

142 DHS, 'DHS's role in state and local fusion centres is evolving', December 2008.The 'Implementation Plan for the Information Sharing Environment' indicates that "that the federal government will promote the establishment of a nationwide and integrated network of state and major urban area fusion centres to facilitate effective terrorism information sharing. This network of fusion centres would house federal, state, and local law enforcement and intelligence resources to provide useful sources of law enforcement and threat information, facilitate information sharing across jurisdictions and functions, and establish a conduit among federal, state, and local agencies".

143 President of the United States, 'National Strategy for Homeland Security', May 2010, p. 28.

144 Ecorys, 'Study on the competitiveness of the EU security industry', November 2009, p. 49.

145 This act reduces the risks to providers that are (normally) associated with the deployment of innovative products. At the same time, through the certification processes, a 'seal of approval' is provided that serves as an indicator of performance of products and services. In turn, this approach has a broader impact as it contributes to the 'creation of a value' associated to the 'quality' of security provided by higher performance products and services. Source: Ecorys 2009.

9.3 The US framework regarding standardisation and conformity assessment

9.3.1 The standardisation framework

Standardisation has a long history in the US as already in the 19th century the first standards were developed. More attention was paid to standards in the beginning of the 20th century especially due to the need of more accurate measurement. It was however not the federal government, but the private industry sector which was the driving force behind standard development.[146] During the last century this situation in fact did not change: private initiatives are still the main developers of standards, although also the government is involved in a supporting role.[147]

The US standardisation system is in fact a decentralised 'bottom-up' system and very market-oriented. The private sector develops all kinds of standards (voluntary industry standards) which are needed for their operations. There exists a wide variety of (groups of) organisations, like trade associations, engineering and professional societies, NGO's, academia and standards developers. These standards-setting organisations normally work in a quite transparent manner, with transparent procedures, open committee meeting, appeal procedures and a 'balanced' representation.[148] However, it should also be noted that some of the standards-setting organisations also dominate or control an entire industry.[149]

There are approximately 600 individual standardisation groups or organisations active in the US (private sector standardisation groups - SDO's).[150]

One of the main coordinating bodies is the ANSI, a private body.[151] ANSI reviews the voluntary industry standards which are developed and determines (on specific criteria) whether these voluntary standards become American National Standards (ANS). In 2009 there were approximately 9,500 ANS'. Beside that they accredit SDO's (at the moment approximately 225 SDO's have a ANSI accreditation).[152]

> **The American National Standards Institute** (ANSI, since 1918) is one of the main representatives of 'private sector voluntary standardisation systems' in the US and is the official US representative to the ISO (the International Organization for Standardization). One of the major tasks of the ANSI is the accreditation of the standards developers, the certification bodies and technical advisory groups (TAGs) to for example the ISO and the International Electrotechnical Commission (IEC). Beside that they also accredit the procedures of standards developing organizations, product certification programmes and personnel certification programmes, etc.[153]As 'umbrella' organisation they are important for standardisation in general, but less for standardisation of security equipment.

---

[146] Companies like Ford saw the advantage of mass production and standardisation. Big efforts on standardisation were made by the US government during World War I.

[147] See for a more elaborate review: U.S. Congress, Office of Technology Assessment, Global Standards: Building Blocks for the Future, TCT-512, Washington, DC: U.S. Government Printing Office, March 1992.

[148] US Department of Transportation, 'Voluntary industry standards and their relationship to government programs', 1993, p. 10.

[149] See previous footnote, p. 24, e.g. the SAE and the ABS.

[150] Purcell, D.E. strategic Standardisation 2008, http://www.strategicstandards.com/Perspectives.html; see also: Thomas, J., 'International Standards and Trade', presentation July 9 2009. Approximately 20 of these SDO's develop 90% of all the standards.

[151] NIST: "The National Technology Transfer and Advancement Act gives NIST the role to coordinate Federal, State, and local standards activities and conformity assessment activities with private sector standards activities and conformity assessment activities, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures", see: http://www.standardsportal.org/usa_en/standards_system/government_use_standards.aspx.

[152] ANSI, http://www.ansi.org/standards_activities/domestic_programs/overview.aspx?menuid=3.

[153] ANSI, http://www.ansi.org/about_ansi/accredited_programs/overview.aspx?menuid=1 and https://www.ansica.org/wwwversion2/outside/PROgeneral.asp?menuID=1, see also: ANSI, the United States Standards Strategy (USSS), 2005.

9.3.2 *The role of the US federal government*

Beside the above mentioned private dimension also the US government plays an important role in standardisation. This role however has multiple dimensions.

First of all they participate in the development of voluntary standards. Main drivers for these activities are the National Technology Transfer and Advancement Act (NTTAA) and an OMB Circular.[154] The NTTAA requires US federal agencies to adopt as much as reasonably possible the existing voluntary (private) sector standards and as a result try to limit the dependence on in-house 'government' standards.[155] The OMB Circular states e.g. that:

- All federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical (under consideration 6);
- Agencies must participate in the development of voluntary consensus standards when consultation and participation is in the public interest and is compatible with their missions, authorities, priorities, and budget resources (under consideration 7);
- Agency support provided to a voluntary consensus standards activity must be limited to that which clearly furthers agency and departmental missions, authorities, priorities, and is consistent with budget resources. ( ) Normally, the total amount of federal support should be no greater than that of other participants in that activity, except when it is in the direct and predominant interest of the Government to develop or revise a standard, and its timely development or revision appears unlikely in the absence of such support (also under consideration 7).

This participation gives an important drive for the development of voluntary standards. The US government may also contribute to the technical underpinning for standards.[156]

Secondly, the government also give a 'push' in the use of these regulation, especially by incorporation of the voluntary standards in the US federal law, which may range from product and food safety to telecommunications and security.[157] Another push factor is the explicit use of and request for certain standards in the public procurement procedures. Private companies which participate in these tender procedures have to comply with these standard requirements.

A third role for the US government is of course the representation of the US in the international field of standardisation (WTO, ISO, etc.).

9.3.3 *The Conformity Assessment framework*

The same decentralised 'bottom-up' structure regarding standards can be found in the conformity assessment procedure (CAC). In general the CAC-system is the same as anywhere else in the world: based on the risks associated with non-compliance the shape of the conformity assessment procedure is determined. For example, in case of high risk related to non-compliance, the need for an independent and rigor assessment by a third party is high. If risks are low, the manufacturer himself can do the assessment. The right balance between risk and costs has to be found.[158]

---

[154] The National Technology Transfer and Advancement Act of 1995, Public Law 104–113; US Office of Management and Budget (OMB), White House, OMB Circular A-119.

[155] See also: NIST, http://gsi.nist.gov/global/index.cfm/L1-5/L2-44/A-331.

[156] NIST, http://www.standardsportal.org/usa_en/standards_system/government_use_standards.aspx.

[157] An overview is given by the NIST: http://gsi.nist.gov/global/index.cfm/L1-5/L2-44/A-331.

[158] Gordon Gillerrman, 'Making the Confidence Connection: Conformity Assessment System Design', 2005.

The US conformity assessment system is decentralised and based on cooperation between both public and private-sector players. It is the responsibility of the private sector itself to shape and to agree upon and the methods and requirements how (non-) compliance to the common standards are assesses. In the US the following private players have a role: [159]

- **US industry**; the US industry plays an important role in determining the requirements of the conformity assessment system, which are often laid down in voluntary conformity assessment programs related to the voluntary industry standards;[160]
- **Conformity assessment bodies (CAB)**; these bodies arrange the certification, testing, and inspection of (product) requirements. In the US there are several of these conformity assessment bodies, which often cover multiple (related) industries. To illustrate this: for toys there is only one CAB, while for electrical engineering there are four. It is not mandatory for CABs to be accredited, but often accreditation is required by their clients;[161]
- **Accreditation bodies**; these bodies assess the competence of conformity assessment bodies (testing labs, inspection bodies, certification bodies, etc.), to make sure that these bodies are for example independent and follow the right procedures. The ANSI also provides accreditation of conformity assessment bodies and besides that promotes and facilitates the US conformity assessment system.[162]

Like in the standardisation framework the US government is again a partner for the private sector regarding the development of voluntary conformity assessment procedures. Beside that, US regulatory bodies also determine in certain regulation the required level of conformity assessment in order to verify whether regulations are met or not. In principle, all these regulatory bodies have the competence to determine the required level of conformity assessment (assessment by a first, second or third party) and the authorized conformity assessment bodies. The same is true for US procurement agencies and their procurement requirements.[163]

As a result the conformity assessment system is a decentralised system with strong roles for private players, like the industry itself (trade associations, engineering and professional societies, etc.), conformity assessment bodies and accreditation bodies. They shape and determine in fact the whole system of conformity assessment requirements. In this system, the US government (consisting of many different bodies and agencies) is in fact more a 'partner' for the private sector than a regulatory authority. The government is part of the conformity assessment system (as a participant) instead of having a control role.[164] There is also no direct conformity assessment policy from the government. The ANSI laid down some guiding principles and definitions in the *National Conformity Assessment Principles for the United States.*[165]

9.4 Standardisation conformity assessment procedures for security equipment

Both the standardisation and conformity assessment processes for security equipment can be mirrored in the general standardisation process and do not differ much from the systems described above. However, given the fact that it is a very decentralised process, the standardisation approaches may differ per sector and or SDO.

---

159 ANSI, http://www.standardsportal.org/usa_en/conformity_assessment/key_organizations.aspx.
160 See: http://www.standardsportal.org/usa_en/resources/sdo.aspx.
161 See: http://www.standardsportal.org/usa_en/resources/cab.aspx.
162 For some examples, see: http://www.standardsportal.org/usa_en/conformity_assessment/3party_conformity_assessment.aspx.
163 ANSI, http://www.standardsportal.org/usa_en/conformity_assessment/key_organizations.aspx.
164 ANSI, http://www.standardsportal.org/usa_en/conformity_assessment/conformity_assessment_faq.aspx.
165 ANSI, http://www.standardsportal.org/usa_en/conformity_assessment/conformity_assessment.aspx.

9.4.1 *Private sector involvement*

As mentioned above there are approximately 600 private sector standardisation groups active in the US, of which some also deal with security equipment. These groups may vary from trade associations (like the American Petroleum Institute – API and the Aerospace Industries Association – AIA)) to professional societies (like the American Society of Automotive Engineers - ASAE) and general membership organisations (like the National Fire Protection Association – NFPA). Given the decentralised approach it is difficult to identify all the organisations which are involved with the (development and enforcement of) standardisation and conformity assessment procedures, especially in relation to the security threats which have been identified for this study.

> **The North American Reliability Company** (NERC) is one of the standard-setting organisations in relation to the protection of critical infrastructure, as they develop standards for the reliability of the bulk power system.[166] They are an accredited body and are also responsible for the independent assessments of the reliability and conformity and entitled to impose fines in case of non-compliance. Security standards for supply chain and container security on the other hand are developed in a quite different way. The US Customs and Border Protection (CBP) set up a public-private partnership (**Customs Trade Partnership Against Terrorism** - C-TPAT) in which public and private actors work together to improve the baseline security standards for supply chain and container security.[167]

These examples illustrate that there does not exist a uniform approach for standardisation and conformity assessment procedures. All these organisations have developed specific industry standards and conformity assessment procedures within their own organisational setup.[168]

9.4.2 *Role of the US government*

The Department of Homeland Security generally follows the policy lines that are given in the NTTAA and the OMB Circular: they are a partner for the private security equipment industry and participate in the voluntary standardisation groups, more specifically in standardisation groups where they have a specific priority or specific expertise regarding the homeland security. They try to assure that the needs and priorities that the US government has regarding homeland security find their way in the standardisation processes.[169] The same applies for the conformity assessment procedures.

Compared to other standardisation areas with less 'national importance', the US Government (the DHS) follows a more focussed approach for issues related to homeland security. They try to focus on specific key areas and deploy if necessary significant resources into the standardisation process in order to get things done. Standardisation is seen as an important method to realise certain objectives regarding homeland security priorities.[170]

This more focussed approach is based on the Homeland Security Act 2002 which states that the DHS (i.e. the Office of Science and Technology - S&T) has to "*establish and maintain performance standards ( ) and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies*". Beside that S&T has to "*establish and maintain a program to*

---

[166] NERC, http://www.nerc.com/page.php?cid=2|247; the North American Energy Standards Board develops the general standards.

[167] CBP, http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/port_security/securing_us_ports.xml; see also: http://www.barnesrichardson.com/?t=40&an=7077&format=xml&p=3734.

[168] For example: the AIA states they approximately 2,800 National Aerospace Standards have been developed, while the NFPA developed approximately 300 standards. The NERC developed approximately 100 standards.

[169] Interview with Mr Gordon Gillerman (NIST, co-chair DHS), d.d. June 8, 2011.

[170] Interview with Mr Gordon Gillerman (NIST, co-chair DHS), d.d. June 8, 2011.

certify, validate, and mark or otherwise recognize law enforcement technology products that conform to established standards".[171] These standards should, according the Homeland Security Act, be in accordance with the National Technology Transfer and Advancement Act[172], which requires US federal agencies to adopt (if possible) private sector standards and as a result limit the dependence on in-house standards.[173]

One of the major partners for the DHS and the Department of Justice (DOJ) regarding standardisation of security equipment is the National Institute of Standards and Technology (NIST, part of the US Department of Commerce).

The National Institute of Standards and Technology (NIST, part of the US Department of Commerce) covers a whole range of services, like weights and measures, calibrations, laboratory accreditation, measurement services and also standardisation. They carry out these services for a broad number of 'subject areas': from nanotechnology and bioscience to physics and public safety/security. Regarding standardisation (as the umbrella term) they are, together with others, involved with the technical standards, the US conformity assessment system, the US accreditation system and the metrology.

The NIST also designs and assists in the implementation of homeland security related conformity assessment programs.[174] The NIST runs several programmes regarding public safety and security, for example:

- X-ray security screening standards for Homeland Security;
- Instrument standards for the detection of hazardous chemical vapours;
- Urban Search and Rescue Robot Performance Standards;
- Metrology and Standards for Canine Olfactory Detection of Explosives;
- Development of NIST Standard Reference Materials for Trace Explosives Detection;
- Measurement Methods and Standards for Public Safety and Security;
- Development of Standard Test Methods for Emergency Response Robots.

9.5 Anti-terrorism technologies: the US SAFETY Act

Pertaining to the conformity assessment and certification procedures specific attention should be paid to the 'Support Anti-terrorism by Fostering Effective Technologies Act' of 2003 (SAFETY Act). As mentioned above, the main purpose of the act was to limit the liability of developers of anti-terrorism equipment, but at the same time the market may perceive this as a 'seal of approval' from the DHS that the technology meets certain market requirements. This results *de facto* in a conformity assessment and certification procedure, although the scope of products is limited to 'terrorism'.

9.5.1 Background of the US SAFETY Act

Occasion and purpose of the SAFETY Act

After the 9/11 attacks the US government wanted to stimulate innovation and R&D in technologies which would protect US citizens against acts of terrorism. However, one of the main problems in this field of technology development appeared to be the liability risks for manufacturers. The threat

---

171 The Homeland Security Act of 2002, public law 107-296, sec. 232.
172 The National Technology Transfer and Advancement Act of 1995, Public Law 104–113.
173 NIST, http://gsi.nist.gov/global/index.cfm/L1-5/L2-44/A-331.
174 Gordon Gillerman, 'Conformity assessment practical implications', (InterAgency Committee on Standards Policy), June 2007.

of liability claims reduced the incentives for market parties to invest in homeland security equipment and to bring it to the market as noted by Carafano (2008):[175]

> Due to the 9/11 attacks there originated a series of lawsuits by victims over the failure to prevent the terrorist attacks and the liability of involved public and private organisations. These lawsuits requested that these organisations should be held responsible for not preventing the attack and that they should pay for the occurred damages. The US government took a number of measures, including legislation which limited the third-party liability of for example some airlines, the port authority, the city authority and some airports. Beside that, also the insurance premiums for terrorism risks increased very strongly resulting in very expensive liability insurances. Carafano points out that "many companies proved hesitant to market anti-terrorism technologies because of two concerns: the costs of potentially devastating jury verdicts should the technologies fail and scarcity of adequate liability insurance".[176]

Given the fact that the US government saw severe positive externalities for innovative (and unproven) security equipment in order to protect the US homeland, they came up with the Support Anti-terrorism by Fostering Effective Technologies Act' of 2003 (SAFETY Act) to solve this market failure.

The main purpose of the SAFETY act is to reduce the liability risks and/or create liability protections for manufacturers and distributors of anti-terrorism technologies, which are sees as very important for the protection of the US homeland security.[177,178] Levin (2004) points out that the act was quite controversial and that the purpose of the act was questioned, as opponents saw it as an attempt to reform tort law, third liability and the government contractors defence:[179]

> The discussions around the SAFETY act stand in a much broader legal discussion regarding the liability of government contractors. The Government Contractor Defence is a common law defence used in lawsuits that makes government contractors (to some extent) immune for liability claims. Reason for this liability defence is related to the fact that otherwise the government has to paid much higher procurement prices (including a risk premium) and that manufacturers often follow procurement requirements by the government (especially in the case of defence equipment).[180] Despite some different interpretations of the exact effect of the SAFETY Act on the Government Contractor Defence, the DHS explains it that certified products and services (under the SAFETY Act) will be successfully covered by the defence.[181]

Scope

The liability insurance (see below) which is covered by the SAFETY Act is related to '*qualified anti-terrorism technologies deployed in defence against or response or recovery from an act of terrorism*'.[182] What is 'an act of terrorism' is not well defined, as the act defines it as "any act that

---

175 Carafano, J.J., 'Fighting terrorism, addressing liability: a global proposal', Backgrounder, published by the Heritage Foundation, May 21, 2008, p. 1-2.

176 Carafano (2008), p. 1-2.

177 Taylor, A.C., 'Government contractors: above the laws of war?', Public Contract Law Journal, Volume 35 (2), p. 281-295, Winter 2006, p. 286.

178 The US Congress formulated it in 2002 as a way "*to ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies from developing and commercialising technologies that could save lives*". Source: Levin, A.M., 'The SAFETY Act of 2003: implications for the government contractor defence', Public Contract Law Journal, Volume 34 (1), p. 175-205, Fall 2004, p. 176-177.

179 Levin (2004), p. 177-178.

180 Taylor (2006), p. 284-285.

181 Levin (2004), p. 189.

182 SAFETY Act 2002, Sec. 864 (3).

the DHS Secretary determines to meet certain requirements".[183] Levin points out that the exact scope therefor lies in the discretion of the DHS Secretary.[184]

Regarding the scope of technology the DHS includes "any qualifying product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause".[185]

9.5.2 *Key components of the SAFETY Act*

There are two main protection procedures included in the SAFETY Act: **designation** as a 'qualified anti-terrorism technology result in a different level of protection and will be discussed below.

Designation as a QATT

The act gives the DHS has the authority to designate certain technologies as a QATT. Technologies which have been tested and used before in operation can apply for a 'normal' designation. For this designation, certain requirements have to be met.

> The SAFETY Act (Sec. 862) determines seven requirements for this designation: (i) prior United States Government use or demonstrated substantial utility and effectiveness; (ii) availability of the Technology for immediate deployment; (iii) the potential liability of the Seller; (iv) the likelihood that the Technology will not be deployed unless SAFETY Act protections are conferred; (v) the risk to the public if the Technology is not deployed; (vi) the capability of the Technology as demonstrated by performance in scientific studies; and (vii) the effectiveness of the Technology in defending against Acts of Terrorism.

The most important benefit for manufacturers is that designated technologies receive a 'liability cap' for third-party claims in case of a terrorist attack.[186] Another benefit is the exclusive jurisdiction for suits in federal courts.[187] The designated technologies are published online.[188]

For technologies which have not been (field) tested or used in a operational setting there exists the 'Developmental Testing and Evaluation Designation' (DTED). Often this type of technology is very promising, but still in a prototype phase and for example not tested in 'real' circumstances. The SAFETY Act offers for these experimental technologies some liability protection, but limited.[189]

Certification

A higher level of protection can be obtained when the QATT is also certified and placed on the 'Approved Product List for Homeland Security'.[190] These technologies are more 'mature' (tested, substantial use, high reliability, etc.) compared to designated technologies. The DHS should in this case 'shall conduct a comprehensive review of the design of the technology and determine whether it will perform as intended, conforms to the applicant's specifications, and is safe for use as

---

183 An act should be (i) unlawful, (ii) cause harm, and (iii) use of weapons/other measures. See Section 865 under B.

184 Levin (2004), p. 199-200.

185 SAFETY Act 2002, Sec. 865 (1). See also: DHS website (retrieved August 2011): https://www.safetyact.gov/jsp/faq/samsFAQRead.do?action=ViewPublished&samsFaq_FaqId=23.

186 The act determines that "the seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies" *Sec. 864 (a) (2).

187 Levin (2004), p. 179.

188 An overview can be found here: (retrieved August 2011): https://www.safetyact.gov/jsp/news/Awards.jsp.

189 DHS website (retrieved August 2011): https://www.safetyact.gov/jsp/faq/samsFAQRead.do?action=ViewPublished&samsFaq_FaqId=57.

190 The list can be found here: https://www.safetyact.gov/jsp/news/Awards.jsp.

intended'.[191] Of course the applicant has to provide necessary information to the DHS (e.g. safety and hazard analyses).

For certified technology, the manufacturer has in case of a lawsuit a 'rebuttable presumption that the government contract defence is applicable and that the manufacturer is not liable for damages relating to the terrorist attacks.

9.5.3 The designation and certification procedure

The procedures for designation and certification are more or less similar and can be applied in two parallel procedures. However, certification is not possible unless the technology is designated.[192] The application process consists of the following steps, which are dealt with electronically.[193] Overall, it is quite an interactive process, with direct interaction between the applicant and the DHS.[194] The whole process is free of charge:

- **Filing of the application.** The first step is to file the designation application and to start the official procedure. In this phase the DHS wants to receive some background information of the technology, e.g. a brief description of the technology (max. 2 pages), including its principal elements, subsystems and components. Important elements are also the 'past and on-going procurements' (e.g. procurements by the military forces, federal government, foreign governments, etc.) and information regarding the available liability insurances (does the market offer only extraordinary high liability?).[195] For certification the applicant has to provide additional information on the performance and whether it works as intended. This performance should be supported with for, example, test data, quality control plans, etc.[196] For first-time applicants there exists also a pre-application phase, in which they will be guided in filling in the application form and providing the right information;
- **Initial notification.** The DHS has to provide within 30 days after the application a notification whether the application is (in)complete and will be reviewed and evaluated. If applicable, applicants have then the chance to complete their application;
- **Review process.** The third phase is the review phase in which the DHS assesses whether the technology will fall under the scope and protection of the SAFETY Act. The DHS has a broad own discretion as they may "consider any scientific studies, testing, field studies, or other experience with the technology that he deems appropriate and that are available or can be feasibly conducted or obtained, including test results produced by an independent laboratory or other entity engaged to test or verify the safety, utility, performance, in order to assess the effectiveness of the technology or the capability of the technology to substantially reduce risks of harm". In case of prior use of the technology in federal, state or local government agencies, the review may be (partly) based on their experience. The review process is carried out by approximately 400 experts with e.g. economic, chemical, cyber, biological or explosive

---

191 CFR, Title 6 (Domestic Security), Part 25.9.

192 Levin (2004), p. 182.

193 This is the main process, the regulation also provides opportunities for 'block designations' and 'block certification' procedures, which are based on predetermined technical criteria.

194 The procedure is described extensively in the CFR, Title 6 (Domestic Security), Part 25.6. This section is primarily based on this source.

195 See for the designation form: https://www.safetyact.gov/jsp/attachment/samsAttachmentDownload.do?action=getStreamInfo&attachmentId=4&attachmentName=10008_Application_for_SAFETY_Act_Designation.pdf.

196 See for the certification form: https://www.safetyact.gov/jsp/attachment/samsAttachmentDownload.do?action=getStreamInfo&attachmentId=5&attachmentName=10007_Application_for_SAFETY_Act_Certification.pdf.

expertise. Every application is reviewed by five reviewers (three technical and two economic experts);[197]

- **Final notification.** Within 90 days after the initial notification the DHS will decide whether (i) the application is approved, (ii) additional information is needed, or (iii) the application is denied. The DHS will also determine the designation and certification period (five to eight years, after that it can be renewed). Again, the level of own discretion of the DHS is quite strong, as the decision is final and (in principle) not subject for additional review.

The average duration of a designation or certification procedure was 113 days in 2010, compared to 163 days in 2004/2005.[198]

9.5.4 *Effects of the SAFETY Act*

Despite a lot of criticism regarding the design of the scheme (definition, scope of protection) and uncertain legal discussions (interpretation of past jurisprudence, acceptance of the government contractor defence by courts, etc.),[199] the SAFETY Act appears to have found its way in the market. The DHS claims that the program "*continues to be very popular with the private sector*"[200].

Some statistics

The claim of private sector popularity of the SAFETY Act program is to some extent confirmed by the application data. The SAFTETY Act had quite a slow start in terms of designations and certifications. The number of full applications was quite low at the beginning and the first certifications were only provided in June 2004, resulting in quite some criticism on the DHS and the measure as a whole.[201] In 2004/05 108 applications were filed, almost the same number as in 2006 (104). Since 2007 the number of applications doubled to 212 in 2010 (2009: 218).[202] This improvement is most likely related to the review of the designation and certification process in the first half of 2006.[203]

Over the period 2006-2010 approximately two-thirds of the applications have been made by small and medium sized enterprises. In 2010 for example small enterprises were responsible for 118 out of the total 212 applications.[204] Since 2004 approximately 440 technologies have been designated as a QATT[205], and approximately 170 technologies were certified.[206]

DHS seal of approval?

Although the main objective of the SAFETY Act was to limit the liability risks for manufacturers of homeland security technology, the DHS designations and certifications are also used as a 'marketing tool' for signalling the expertise of a company and in that sense a conformity assessment procedure for a specific range of security products.

---

197 DHS, 'SAFETY Act', PowerPoint presentation by the DHS, dated May 2011. In other presentations (undated) the DHS stated that 420 reviewers were involved.

198 DHS, 'SAFETY Act', PowerPoint presentation by the DHS, dated May 2011. In other presentations (undated) the DHS stated that 420 reviewers were involved.

199 See the discussions raised by Levin (2004) and Taylor (2006).

200 Benda, P., "Unlocking the SAFTEY Act's potential to promote technology and combat terrorism', Testimony of Acting Deputy Under Secretary of the DHS, May 2011. See: http://www.dhs.gov/ynews/testimony/testimony_1306419295690.shtm.

201 Levin (2004), p. 200-201.

202 Benda (2011).

203 Greenberger, M., 'Teaching new dogs old tricks: reshaping the department of homeland security's technology development infrastructure', Jurimetrics, volume 47, p. 281-296, spring 2007, p. 286-287.

204 Benda (2011). Small is defined here as a company with less than $ 50 million turnover, medium is between $ 50 million and $ 1 billion. Large enterprises have more than $ 1 billion turnover per year.

205 Benda (2011).

206 DHS website, Approved Product List for Homeland Security, calculation by Ecorys.

Levin points out that "although there is no direct evidence that the SAFETTY Act was intended [by Congress] to alter the competitive balance between technology providers, ( ) the certification and listing could be a good marketing for vendors".[207] She refers also to other sources which points out that "the DHS designations and certifications will likely be perceived by potential customers as DHS' seals of approval".[208] This is also indicated by Biagini, who argues that the DHS designation or certification will create a competitive edge in the homeland security market because customers of designated or certified companies 'offer' their clients (to a certain extent) immunity for tort laws. He also expects that federal, state and local authorities will try to procure DHS-approved technologies.[209] In more recent literature there is a little evidence on how this worked out in practice. Greenberger (2007) points out that the DHS listing amounts to a 'good housekeeping seal of approval'[210] and Pavlick (2006) indicates that several organisations (e.g. the US army) stimulate companies to receive the DHS approval for their procured technologies. Besides that, also private companies indicated that "in the future they will require prospective contractors (when relevant) to have a SAFETY Act designation/certification as a precondition to bidding or offering to perform on a contract".[211] More illustrative evidence can be found in press releases and on company websites. The designation and/or certification of technologies by the DHS is made very explicit, and is presented as an important competitive advantage towards other market players.[212]

9.6 Comparison EU-US framework: main findings and issues

When we look at the system of standardisation and conformity assessment in the US and the EU, two important observations can be made.

First, it is assessed that the general approaches between the US and the EU differ fundamentally. The US relies fully on a system of voluntary standards which are developed in the private sector. The standards and conformity assessment agreements are based on a consensus between trade associations, engineering and professional societies, etc. The same situation is applicable for the conformity assessment procedures. These procedures are developed and negotiated on a decentralised level between market players. Given the fact that there are more than 600 standard development organisations it is clear that also the set-up of the conformity assessment procedures differs per organisation.

Secondly, in this decentralised bottom-up approach the US government mainly acts as a 'partner' (and not regulator) towards these standard development organisations. Depending on the specific public interest the government agencies contribute to the development process (e.g. with physical resources, technical expertise, etc.). This involvement is mainly triggered by the NTTAA which forces federal agencies to use voluntary industry standards instead of developing 'own' governmental standards. The NTTAA gives federal agencies the room to be involved in the development process when there is a public interest for it. In case of homeland security, the involvement and alertness of the US government (DHS) may be stronger, but in principle they follow the private, decentralised approach.

---

207 Levin (2004), p. 201-202, based on Tanenbaum, W.A., 'Updating key contract terms in business process, IT and offshore outsourcing, in: The outsourcing revolution, 2003.

208 Levin (2004), p. 200-201, footnote 190.

209 Biagin, R.B., 'Involving the SAFETY act: a matter of corporate responsibility and competitive edge', The Procurement Lawyer, volume 39 (3), p. 23-26, spring 2004, p. 24.

210 Greenberger (2007), p. 286.

211 Pavlick, J.J., Locaria, D.N., 'Final SAFETY Act rule resolve some questions, generates others, and creates important procurement linkage to the SAFETY Act', the Procurement Lawyer, Volume 42 (1), fall 2006, p. 28.

212 See for example Lockheed Martin (http://www.lockheedmartin.com/products/CriticalInfrastructureProtection/index.html and AKAL Security (http://www.akalsecurity.com/safetyact).

These first two observations show a strong difference with the EU, where there is more a top-down approach: national standardisation institutes take the lead in developing national standards and conformity assessment procedures. Market players are involved of course, but their role is less stringent than in the US.

Of course there are disadvantages of this US bottom-up approach (risk of lack of coordination, risk of lack of vision, risk of one party dominance, conflicting stakeholder objectives, severe investments in participating in these standard development groups, risk that the market does not recognise certain security threats and the need for standardisation, etc.), but in general this system approach is seen as an advantage due to cost savings (interoperability, avoiding duplicative R&D and compliance costs, etc.) and competitive and market advantages (ensuring standards meet business needs, understanding of issues facing industry, reliability, and market acceptance, etc.).[213]

A third observation is that since the 9/11 attacks, there is a strong consciousness that the US faces severe security threats. As a result the attention for homeland security is very strong. This is illustrated with the institution of the DHS in 2002 and the granting of serious federal budgets (€ 41.7 billion for the DHS in 2010). Additionally, the DHS is since 2006 working on further integration of local, state and federal intelligence and information sharing in the fusion centres. Compared to the fragmented system in the EU this centralised approach may create a fundamental competitive advantage (integrated approach, less fragmented regulator system, role of the government as launching customer, etc.).

A final observation can be made on the SAFETY Act. The main objective of the SAFETY Act (*de jure*) was to limit the liability risks for manufacturers of homeland security technology. However, *de facto*, this procedure results in a conformity assessment procedure for a certain type of security equipment and services (only related to anti-terrorism). This 'seal' is used by manufacturers to indicate their 'unique' position on the market, and also expected to be requested more and more by public and private purchasers of security technology.

[213] NIST, Summary of the Responses to the National Science and Technology Council's Sub-Committee on Standards Request-for-Information, 'Effectiveness of Federal Agency Participation in Standardization in Select Technology Sectors', December 8, 2010.

Part IV – Options for enhanced conformity assessment and certification of security products

10 Outline approaches for EU-wide conformity assessment and certification of security products

10.1 Introduction

The following discussion is centred on developing possible options to enhance existing frameworks for conformity assessment and certification (CAC) of security products within the EU[214]. In this regard, it is important to mention that the discussion does not deal in any depth with issues related to the existence, or otherwise, of standards for security products. The issue of standards for security products is outside the scope of the present study but it is nonetheless largely self-evident that any discussion of options that would move towards greater harmonisation of existing CAC systems within the EU – or the development of new EU-wide systems – will go hand-in-hand with the development of appropriate (harmonised) standards. Some comments are provided in the following sub-section.

10.2 Development of common EU standards for security products

EU standards (related to security characteristics) do not exist for many categories of security equipment. Further, even where EU standards exist they may be less well accepted by regulators and/or by the market than national standards. This implies the need to develop common EU standards for a wide range of security products (or, at least those regarded as a priority by EU and national authorities). However, acceptance of common EU standards – whether entirely new standards or based on harmonisation of existing (national) standards – depends on those standards meeting the exigencies of national authorities and regulators, manufacturers of equipment and their customers, and other relevant parties (e.g. insurers, private citizens) in different markets within the EU. In the absence of agreement on common standards, it is unlikely that Member States would (voluntarily) agree to any procedure for mutual recognition of certification/approval of security products.

Following from the above, even if common standards for security products are agreed upon, it cannot be assumed that they would 'quasi automatically' lead to an end of market fragmentation. Past experience shows that, even within a single jurisdiction, it can take different certifying bodies many years of regular consultation to determine how to interpret standards (and conformity assessment schemes). It is not unreasonable to expect that such process will take even longer when they require agreement across different jurisdictions and languages. This may be reinforced by the fact that certifying bodies that have a dominant position in their national markets may have little incentive to promote effective and efficient interpretation and implementation of standards that contribute to reducing market fragmentation.

A further dimension relating to the role of standards to reduce market fragmentation is that common EU standards are developed in relation to the security performance characteristics of security products (equipment) per se may be insufficient if differences persist in the standards applied to

[214] In this chapter, unless otherwise stated, the term security products may be applied to denote security equipment, systems and services.

larger systems or to services related to the installation, maintenance and operation of security equipment, There remains the risk that common EU product performance standards are 'complemented' at a national level by other rules and requirements that *de facto* act to create or maintain market access barriers. In this regard, a comprehensive approach to standardisation may be required; as is called for by some security product suppliers. Such a 'solutions-based' approach would integrate standards relating, for example, to aspects such as the planning, installation, maintenance and operation (e.g. training of security personnel) into a package of appropriate common 'standards'. In fact, such an approach may be advantageous for EU suppliers of security solutions that gain their competitive advantage over low-cost suppliers of security products (equipment) on their ability to provide a client with a more complete service that includes such additional elements.

Comments:

In referring to common EU standards, this does not imply European Standards developed by CEN and affiliated organisations (CENELEC, ETSI). For some product categories it is quite feasible to envisage the development of (harmonised) European Standards and such standards have been developed in related areas (e.g. harmonised norms exist in the area of fire protection (security electronics) as required/referred to under the Construction Products Directive). The possibility to apply European Standards for security products needs to be set against the fact that:

- Standards relating to the performance characteristics and associated testing criteria and procedures for some categories of security equipment/products are often classified/secret information, which would reduce the possibility for developing European Standards using 'open' processes and at the level of detail required for CAC of security performance characteristics of security technologies/ equipment;
- Processes for the development of 'consensus-based' European Standards may not be sufficiently rapid to address actual needs for new standards to meet evolving security threats and corresponding technology developments.

In developing common EU standards it needs to be recognised that the market for security products is highly diverse. Performance requirements (technical and operational) for different sectors/environments and for different users may vary significantly; further, differences in national security situations (e.g. threat scenarios) may also imply differences in performance requirements. These differences in performance requirements may necessitate the development of 'variable' performance standards that reflect the requirements of different sectors/environments, users and national situations. In this respect, rather that setting minimum performance thresholds (and pass/fail tests of conformity) it may be more appropriate to use standardised methods for measuring and categorising security performance criteria. This would permit the performance capabilities of equipment to be graded, while allowing relevant authorities – and procurers/users – to specify the performance grade required for security equipment used in different situations/markets. In this regard, existing EU regulations (e.g. aviation security equipment) already apply 'variable' standards for some categories of security equipment, albeit in the context of improved detection performance requirements over time. Such an approach would also increase transparency in the market by providing suppliers and customers with an independent and objective evaluation of the performance characteristics of different products (rather than simply a demonstration of conformity with a minimum EU standard). Clearly, this may need to be set against the risk of providing criminals/terrorists etc. with greater information on the level of security provided by different equipment.

As far as possible, a CAC procedure for security products should provide for the demonstration of conformity with all specified (regulatory or other) requirements and specifications within a single procedure. Accordingly, the scope of relevant requirements - and corresponding common reference standards - that may be covered by a CAC procedure for security products is not limited to only security performance *per se*. Other requirements and corresponding standards (including those related to testing and other

conformity assessment methods), the development of which may be an integral part of the implementation of a CAC procedure, may relate to:

- *Generic* requirements (e.g. health and safety, environment, etc.);
- *Supporting* and *interoperability* requirements;
- *Operational* and *integration* requirements;
- *Associated* requirements, linked to general principles (e.g. ethical / societal).

Concerning the final bullet point above, the debate surrounding the use of "security scanners" (otherwise known as body scanners) for screening passengers in the aviation sector provides a clear example of the kinds of ethical concerns that may be raised by the use of security equipment/technologies. The Commission Communication on the use of security scanners at European airports[215], takes the view that "*Under existing technology and safeguards attached to the use of Security Scanner equipment, fundamental rights issues can be dealt with by a combination of technical equipment specifications and operational rules. Minimum standards could be laid down by law*". Further, the Communication states "*Whatever technology and operational safeguards chosen, the modalities for the use of Security Scanners would need to be provided for in binding rules. Member States' authorisations for individual deployment at airports should be based on a thorough assessment of a possible impact on fundamental rights and safeguards available*."

This clearly leaves open the possibility for European legislation that would set standards for security equipment (and the operation of such equipment) related to fundamental rights (e.g. privacy and data protection); though it remains to be seen what standards (and technical specifications) and conformity assessment requirements may in fact be proposed by the Commission. In May 2011, the European Parliament's Transport Committee[216] made clear that if security scanners are deployed "*health and fundamental rights must be safeguarded along with personal data, dignity and privacy*". Moreover, notwithstanding these safeguards, the Transport Committee affirmed that passengers should be given the right to refuse body scanning and submit to alternative screening methods that guarantee the same level of effectiveness while respecting their rights and dignity.

10.3 General framework for assessment of CAC requirements and policy options

In defining possible options for CAC for security products, account needs to be taken of the wide diversity in security threats and corresponding capability and performance requirements; in security products and security technologies, including their level of maturity and complexity; and in security markets, both in terms of economic sectors/activities and categories of customers (institutional, private, etc.), and in the 'drivers' shaping demand. This implies that there are contrasting needs in terms of levels of security (i.e. standards of security performance to be obtained), the corresponding rigorousness of conformity assessment procedures, and the technological sophistication of methods required for conformity assessment.

DIN response to EC Consultation: problems experienced with national CAC procedures

As an illustration of the scope of security products, technologies and/or systems where problems have been encountered due to national conformity assessment and certification procedures, DIN the German Standardisation Organisation provided the following list in reply to the European Commission's "Consultation on an Industrial Policy for the Security Industry"[217]:

---

215 COM(2010)311.

216 See: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20110523IPR19946+0+DOC+XML+V0//EN&language=EN.

217 Source: http://www.sicherheitswirtschaft.din.de/sixcms_upload/media/3442/2011_05_06_Antwortvorlage_PC_Security.pdf.

- **Fire Detection** (products, systems and services);
- **Alarm Systems**: fire, intruder and hold-up alarms;
- **Closed Circuit Television** and **Access Control** areas;
- **Physical access and identity of workers at airports and seaports** (Schengen border);
- **Physical access to Critical Infrastructure**; missing standard and recommendation;
- **Physical and logical access of government employees**; various implementations (e.g. Germany, Netherlands, Italy, Spain);
- **Physical access in fun lines** (e.g. ski arena, soccer stadium); various implementations in the European Alps and various implementation in the big stadiums;
- **e-Gates** at airports (focus airport hubs); various implementations (e.g. Schiphol, Charles de Gaulle, Fraport, Heathrow, Faro etc.);
- **e-Ticketing** in Public Transport; various implementation (e.g. Paris, London, Rome, Milan, Stockholm, Netherlands, Madrid etc.);
- **e-Vehicle Registration** along EU recommendation 2003/127/EC; four implementations in Europe (Netherlands, Serbia, Austria, Slovakia);
- **e-Driving License**; 3 feasibility tests are done (Netherlands, UK, France);
- **e-Metering systems**; missing standard and recommendation;
- **e-Asylum seeker identity**; missing standard and recommendation;
- **e-Emergency data and token** in Europe; missing standard and recommendation;
- **e-Government services**; various implementations (e.g., Germany, Italy, Spain, Portugal, Sweden, Switzerland, Belgium, Finland, Ireland, Austria, Serbia, etc.;
- **e-Health services**; various implementations (e.g. Slovenia, UK, Spain, France, Italy, Germany, Belgium, Austria etc.);
- **Secure ICT infrastructure** in the public domain and in critical infrastructure; missing standard and recommendation;
- **Electronic toll collection** on highways; various implementations (e.g. Switzerland, Germany, Lichtenstein);
- **Identity of professional service provider** (e.g. health professional service); various implementations (e.g. Slovenia, France, Italy, Switzerland, Spain, UK etc.);
- **Mobile communication systems for remote control of ICT systems**; missing standard and recommendation;
- **Mobile terminals for border control** (e.g. in pan-European trains), missing standard and recommendation;
- **Mobile payment**, e.g. based on NFC Cell Phone; missing standard and recommendation.

10.3.1 Characterisation of security market environment

While interaction of the factors indicated above implies a complex set of market conditions, the general situation can be characterised in terms of two contrasting market-product segments that illustrate the differing challenges for any EU initiatives towards conformity assessment and certification:

- **Type-1:** security products and solutions aimed at addressing 'familiar' security situations (security threats or functions) through the application of improved but existing technology. This includes what may loosely be called 'traditional' security equipment (e.g. intruder detection, CCTV, access control, security barriers);
- **Type-2:** security products and solutions addressing 'unfamiliar' or new types of threats that often require the development or application of new technologies and approaches. This latter category may be extended to changes in organisation and implementation of security functions; for example through the automasation of security functions (e.g. border/passport control by eGates rather than border police).This includes what may loosely be called 'new' security

equipment (i.e. corresponding to products/technologies developed primarily to address threats such as terrorism, organised crime, cyber-crime, etc.).

Table 10.1 Main characteristics of market-product segments

	Type-1 (General security products)	Type-2 (High security products)
Threat type	'Continuous' / 'Endogenous' (e.g. ordinary criminal activity). Threats are generally known and their evolution is relatively predictable.	'Disruptive' / 'Exogenous' (e.g. terrorism, organised/ international crime). Threats are often unknown and their evolution is unpredictable.
Products / technology	'Established/mature'. Technology development based on incremental improvements.	'New/immature'. Technology development is in reaction to new threats or market opportunities.
Operational approach (security function)	Handled in traditional way: technology used to assist human security functions.	Trend towards automation of security functions: human activity substituted by machines/systems (e.g. eGates instead of manual border control; body scanner instead of manual body checks).
Demand	Largely market driven.	Largely regulatory driven.
Standards and CAC standards	Existing national standards and CAC (legacy systems) with limited EU-level harmonisation.	No or limited standards and CAC (either at national and EU-level).

10.3.2 Characterisation of policy challenges

Security products are normally subject to some form of national validation and approval/certification procedures. In the absence of mutual recognition, security products must undergo testing, validation and approval/certification procedures in each Member State where the supplier wishes to make their product available. Currently there is no common EU-wide system providing conformity assessment and certification (CAC) of security products; at least in so far as the requirements for such products are not covered by 'generic' requirements (e.g. health & safety, environmental, electro-magnetic compatibility, etc.) or non-security specific legislation (e.g. Construction Products Directive), for which the general EU approach is framed within the New Legislative Framework. Some steps have been taken towards the development of EU-wide systems, for example the ECAC Common Evaluation Process in the aviation sector, though this applies only to certain categories of equipment[218] and stops short of a procedure for mutual recognition of approved/certified equipment[219].

[218] The CEP incorporates Common Testing Methodologies (CTM) for Explosive Detection Systems (EDS) and since 2010 for Liquid Explosive Detection Systems (LEDS) as well. CTMs for Security Scanners and Explosive Trace Detection (ETD) systems are under development.

[219] Under the CEP, participating test centres transmit the results to ECAC. In turn, for equipment attributed an EU performance standard, this is passed on to the appropriate authorities of the ECAC Member States, which can certificate the equipment based on the test results and subsequent attributed Standard. Usually Member States convert a 'pass' directly into a certification, although sometimes an exception is necessary though in case of more stringent national regulations.

As a consequence of the requirement for national approval/certification of security products, suppliers are faced by the administrative burden and the associated costs of complying with multiple national procedures in order to have their products approved/certified within the EU market. These costs may deter suppliers from entering some national markets, hence representing a barrier to the development of a genuine Internal Market for security products within the EU. Further, reduced market access may act to inhibit the development and diffusion of new security technologies and solutions, while undermining the competitive position of EU suppliers. For example, EU companies that develop new technologies to address new threats suffer in comparison to competitors, in particular from the U.S., if their equipment is not as quickly tested, certified and installed as their competitors. Slow and cumbersome CAC procedures in the EU imply that products from EU suppliers arrive with a time lag in export markets; moreover, they can't scale their production as quickly if they have to obtain numerous national certificates. All these factors put them at a disadvantage in export markets ("proof of concept", learning curve effects etc.). At the same time, a system based on individual national testing, validation and approval/certification procedures in different Member State arguably represents an unnecessary duplication of effort and an inefficient use of resources.

For Type-1 products, the main policy challenges stem from the absence of common EU-wide certification of products. Manufacturers and suppliers point the fact that they are faced with *de facto* requirements to separately certify products in almost all EU countries as there is no – or very limited – recognition of certification between countries. In this regard, they argue that certification bodies have been slow to embrace EU-wide solutions that would reduce or remove the need for multiple national certifications. As a consequence, manufacturers and suppliers face the administrative burden and cost associated with multiple certifications of their products which, particularly for SMEs, represents a significant barrier to supplying new markets. Certifying bodies counter that the market demands for national certification are associated more to the lack of acceptance and use of European Standards; either because harmonised European Standards do not exist, are not familiar to market actors, or do not meet specific national exigencies.

For Type-2 products, the range of policy challenges is wider, since there is often a direct link to issues of EU Internal Security, including ensuring minimum security performance levels (and promoting higher ones) and speeding-up the deployment of new technologies and solutions. Here, in combination with the development of common EU standards for performance (and other aspects such as interoperability), a common approach to conformity assessment and certification could contribute to reducing/avoiding the fragmentation of newly emerging market segments in the EU. An EU wide CAC system – based on common performance criteria – should increase market transparency by providing end-users with greater information on the relative attributes of different products and, hence, promote competition.

Table 10.2 Main policy challenges/objectives

	Type-1 (General security products)	Type-2 (High security products)
EU Internal Security Public interest rationale (security of citizens)	[Possible complementarity to Internal Security Policy needs].	Ensure common (minimum) performance levels for security products in the EU. Promote higher performance levels for security products in the EU. Accelerate the deployment of security products/technologies and solutions throughout the EU.
EU Internal Market Market failure rationale (barriers to trade)	Reduce barriers to trade in security products within the EU.	Reduce fragmentation of EU markets for security products within the EU. Promote a 'level playing field' for security products within the EU.
EU Industrial Policy Market failure rationale (market efficiency, technology development, competitiveness)	Reduce the burden of CAC requirements through common standards and CAC procedures.	Reduce the burden of CAC requirements through common standards and CAC procedures. Support the development (and deployment) of new security technologies and solutions by reducing time to market and increasing product diffusion (earlier achievement of scale effects). Create opportunities for introduction of innovative solutions enhancing efficiency and effectiveness of security functions (e.g. through automated approaches). Support export of EU security technologies and solutions.

10.3.3 Characterisation of EU-policy approaches

Reflecting the main challenges faced by companies seeking to introduce innovative technologies and solutions into the security market, two overarching – and inter-related – aims for any possible policy options to enhance existing frameworks for conformity assessment and certification (CAC) of security products within the EU can be identified:

- To reduce the number of (national) conformity assessment procedures necessary to receive approval/certification for the entire EU market;
- To speed-up procedures for testing, approving and certifying new equipment (and new technologies) that are developed – and required – to respond to new security threats (e.g. body scanners).

In deriving possible approaches to address the above aims, a basic consideration is whether the approach should build on existing infrastructure and systems for CAC or whether a dedicated approach is required. For Type-1 products it seems appropriate to build on existing CAC schemes. For Type-2 products that are associated with specific regulatory responsibilities (and expertise) and

require specialist technical expertise, a dedicated CAC scheme and infrastructure is more likely to be necessary.

For Type-1 products, for which there exist performance and other technical standards – albeit differing at national levels – and national infrastructures for testing equipment in many Member States, the outlined approach is as follows:

- **Standards harmonisation:** The first focus for EU policy intervention would relate to the development of harmonised European Standards and the promotion of their use within the market (see next bullet point). The adoption of harmonised European Standards would provide the basis for EU-wide certification, either through mutual recognition of national certification or certification through an approved EU-wide sector scheme;
- **Market recognition of European standards:** The second focus for EU policy intervention relates to the extent of market recognition of products certified as conforming to European Standards. On the one hand, the market may recognise European Standards and duly certified products without the need for further EU intervention; i.e. a voluntary solution is achieved. On the other hand, if there is continued insistence on national certification then additional EU intervention may be justified. This could include non-legislative initiatives to promote recognition of European Standards and EU-wide certification with relevant markets actors[220], which may include encouraging national (and local) administrations/authorities and regulatory bodies to integrate conformity to European Standards in procurement requirements;
- **Regulation:** A legislative approach may be adopted if a market-based solution resulting in common (EU-wide) certification or mutual recognition does not develop. This could take the form of the introduction of specific legislation for security products following, for example, a NLF approach that would prevent Member States from prohibiting the placing on the market of security products that have been certified by a competent (notified) conformity assessment body in another Member State;
- **Conformity assessment and certification:** Notwithstanding whether a market-based or legislative approach is adopted, existing accreditation procedures and conformity assessment infrastructures (e.g. testing laboratories) could be used to provide conformity assessment (testing) services and certification in accordance with the – to be developed – harmonised European standards.

For Type-2 products, consideration needs to be given both to the process of defining EU standards, including those related to testing methodologies and test criteria, and to the overall design of an EU system for conformity assessment and certification. In this regard a number of issues arise:

- **Regulatory approach.** Relevant EU regulatory frameworks can be characterised as either sector-based or product/technology-based:
  - ***Sector-based frameworks*** apply to particular (economic) environment or activity and typically set requirements for the security programmes (procedures and processes etc.); for example, through requiring the designating of security authorities and requiring the Member States to ensure the appropriate security plans are developed. Such regulations may set out specific performance or other technical requirements for security products but typically this is not the case;
  - ***Product-based or technology-based frameworks*****,** define performance or other technical requirements for security products that apply irrespective of the environment in which they are to be used;

[220] These may include not only suppliers and purchasers of security products, but also the insurance sector and other actors involved in the specification of security requirements (e.g. building authorities, constructors, architects, engineers, etc.).

- To date, the main thrust of EU security-related regulations has been of the first type, with regulations orientated towards a particular type of (economic) environment (e.g. aviation, maritime, critical infrastructure, etc.) or activity (e.g. border control, management and transport of hazardous materials, etc.). Accordingly, a sector-based approach for CAC would complement existing sector-based regulatory frameworks but would be limited only to the sectors covered by legislation. A product-based approach to CAC would provide a general system of approval/certification of categories of products but would need to address possible variations in requirements for different sectors/activities. Taking a rather pragmatic approach, from a legislative perspective it would arguably be easier to follow a sector-based approach, since this would enable Implementing Acts – setting out technical requirements and CAC procedures – to be 'attached' to existing sector-based security-related regulations. However, if the overriding concern is to reduce market fragmentation within the EU and across sectors then a product-based or technological-based framework may be preferable, since this would create a single system of CAC for product categories, irrespective of the sector in which they are deployed. This would require new Legislation setting essential (and technical) requirements for categories of security products and may be less rapidly introduced than Implementing Acts attached to existing regulation. However, ultimately, a product based approach could lead to a more harmonised overall approach for CAC.

- **Standards.** A basic principle for CAC is that it should demonstrate conformity to recognised standards (preferably international or European) or other transparent and objective criteria – such as technical regulations – in a non-discriminatory manner. Similarly, when setting performance measurement standards, the measurements or test results should be traceable to recognised (preferably international or European) measurement standards. These criteria pose a number of difficulties with respect to Type-2 products, particularly for new technologies for which recognised standards may not exist. This may be a specific problem where deployment of the product is immediately or imminently required (for example, in response to the evolution of security (terrorism) threats). Furthermore, security performance requirements and associated test criteria can be 'sensitive' (e.g. classified or secret) information, making it more difficult to provide transparency and ensure objectivity while, also, requiring protocols for information confidentiality that may influence the definition of a CAC system;
- **Accreditation.** A common EU CAC system for security products would have to command the confidence and support of Member States throughout the EU, thus enabling the principle of mutual recognition to be accepted (i.e. Member States recognition of certification received from another Member State or, possibly, a central EU Certifying Body). In order for Member States and other stakeholders to have confidence in the CAC system and procedures, adequate and appropriate 'checks and balances' would be required to assure necessary expertise of conformity assessment bodies (e.g. testing laboratories) and to assure that applied conformity procedures are appropriate (e.g. test criteria and methodologies utilised by the laboratories are adequate to demonstrate conformity with the specific technical requirements set for a given product category);
- **Certification.** One of the main aims of a common EU CAC system for security products would be to remove (or at least reduce) the need for multiple national approval/certification of security products. A fundamental question is, therefore, the extent to which national authorities would be prepared to accept the principle of mutual recognition of approval/certification by another Member States. For some product categories it has been indicated that, irrespective of the reliability and integrity of an EU-wide CAC system, Member States may consider that they have an essential obligation to undertake their own national testing and validation of certain categories of security products. One example of EU Regulations 'imposing' mutual recognition is, however, found under EU Regulation 185/2010 with respect to equipment for the screening

of LAGs (liquids, aerosols and gels) in the aviation sector[221]; although it is not certain how this will operate should a Member State raise an objection to an approval/certificate issued by another Member State. An alternatively may be to adopt a more centralised approach with approval/certification being issued by a single organisation subject to specific scrutiny by the EU with, or on behalf of, national authorities.

Table 10.3 Outline EU policy approaches

		Type-1 (General security products)	Type-2 (High security products)
EU Regulatory Approach		Product-based.	Product-based or Sector-based.
Non-regulatory		Initiatives to promote development and market adoption of European Standards.	*[Initiatives to promote development and market adoption of EU standards].* *[Initiatives to support the development of CAC infrastructure and systems].*
Regulatory		*[Specification of EU requirements for security products.]*	Specification of EU requirements for security products (and technologies). Either 'generic' (product category) or in relation to products employed in defined sectors, environments, or activities.
		[Technical regulations (implementing legislation) specifying relevant European Standards]	Technical regulations (implementing legislation) specifying standards / technical specifications / codes of practice.
Standards	**Product**	European Standards: harmonisation of (national) standards for security products.	Specification of common EU standards for security products (and technologies). *[Integrating existing EU or international standards, where available].*
	Testing	European Standards: harmonisation of (national) standards for testing of security products.	Specification of common EU standards for test criteria and procedures. *[Integrating existing EU or international standards, where available]*
Accreditation	**Testing laboratories**	*[EA procedures for accreditation of testing laboratories].*	EU approval of (national) security testing laboratories. *[Eligibility limited to nationally accredited / approved or government-run facilities].*
	Certification bodies	*[EA procedures for accreditation of testing laboratories].*	a. EU approval of (national) security certification bodies. *[Eligibility limited to national administrations].*

[221] § 12.7.3 states that "*Equipment that is approved by or on behalf of the appropriate authority of a Member State to meet the standards as laid down in a separate Commission Decision shall be recognised by other Member States to meet these standards. Member States shall submit to the Commission the name and, upon request, other relevant details of bodies designated to approve equipment. The Commission shall inform other Member States of the bodies*".

		Type-1 (General security products)	Type-2 (High security products)
			b. Single EU security certification body. *[EU Agency]*
Certification		a. Certification by national CABs to European Standards (with mutual recognition).	a. National certification of conformity to EU standards (with mutual recognition).
		b. Certification by sector CABs to European Standards (sector scheme).	b. EU certification of conformity to EU standards.

10.4 Outline approaches and options for EU CAC schemes for security products

Following from the preceding discussion, it is envisaged that at least two different approaches are required to accommodate the diversity of security products:

- **EU CAC for 'general purpose' security products (Type-1).** Intended to cover security products aimed towards 'general' security markets and/or based on comparatively mature technologies (Type-1);
- **EU CAC for 'priority and sensitive' security products (Type-2).** Intended to cover security products aimed either towards 'specific' markets and/or based on comparatively new or innovative technologies (Type-2).

These options are described in more detail in the following sections.

10.4.1 EU CAC of 'general-security' equipment (Type 1)

Product coverage

The aim of this option is to provide an EU-wide CAC system for general security products that are primarily employed to address traditional security threats (e.g. 'ordinary' criminal behaviour); though they may also be utilised as part of measures to address 'high-level' or priority security threats. The system would be intended to provide a common system for testing, validating and certifying compliance with EU (minimum) requirements for the performance of such security products as defined by a harmonised European Standard (EN).

Regulatory approach

As discussed below, the focus of EU policy intervention under this option would relate to the development of harmonised European Standards and the promotion of their use within the market, combined with encouraging EU-wide schemes for common certification and/or mutual recognition.

Certification of conformity with European Standards would *a priori* be 'voluntary' on the part of manufacturers/suppliers, However, compliance with European Standards may be required for certain markets (i.e. for specific market sectors or activities) either as a result of legislation (*de jure*) or other conventions (e.g. guidelines, advice notes, codes of practice, voluntary agreements, etc.) applying to the market that recommend the use of European Standards such that compliance is *de facto* obligatory.

An EU-level legislative approach may be adopted if a market-based solution resulting in common (EU-wide) certification or mutual recognition does not develop. This could result, for example, if national certifying bodies continue to maintain national certifying schemes in such a way as to undermine the development of a common EU wide scheme that removes the need for products to undergo multiple nation conformity assessment procedures. An EU-level legislative approach could take the form of the introduction of specific legislation for security products following, for example, a NLF approach. Such legislation would aim to prevent Member States prohibiting the placing on the market of security products that have been certified as conforming to EU standards by a competent (notified) conformity assessment body in another Member State. Alternatively, legislation could look towards regulating the conformity assessment schemes and organisations.

Comment and assumptions

A regulatory approach based on the NLF may be problematic in so far as EU legislation would relate to 'security performance' rather than the 'safety' aspects of products, which are more normally the subject of EU legislation. Further, it may be questioned whether such an approach is appropriate when the main market (and public policy) concerns are not necessarily about achieving EU minimum performance standards but demonstrating appropriate performance for a particular environment (and associated risk assessment). For the purpose of the assessment of impacts of is Option A it is assumed that if EU legislation is required, such issues may be adequately addressed enabling an EU-wide approach to be implemented.

Standards

NB: It is important to recall – as noted in the introduction to this Chapter (see Sections 10.1 and 10.2) – that the issue of standards for security products is outside the scope of the present study. Accordingly, it is difficult to evaluate if standards-related issues lie behind national certification bodies slow embrace of EU-wide solutions that would reduce or remove the need for multiple national certifications, or whether this provides a 'convenient excuse'. We here outline the underlying assumptions regarding the availability of European Standards (EN) under this option.

From the perspective of developing policy approaches for Type-1 products, the main issue identified by stakeholders concerns the existence and appropriateness of European Standards. European Standards already exist in the area of fire protection (security electronic) and are referred to in the Construction Product Directive/Regulation of the Commission); conformity with these standards – as indicated by the affixing a CE label – is required to sell the product in the EU market. In the area of security products such as intrusion detectors, CCTV surveillance cameras, Access control equipment and other security management systems either no such harmonised standards exist or, where they do exist, are not widely adopted[222]. Consequently, where conformity with performance (and other) criteria is required – either as a result of national regulation or market-based requirements – CAC is undertaken on the basis of national standards, and under different test scheme in many Member States. Accordingly, EU policy intervention is called for in order to promote (or mandate) the development of harmonised European Standards. An 'improved' body of European Standards would provide the basis for 'voluntary' solutions that would remove (or at least reduce) the need for national certification, without the need for specific EU intervention.

[222] Some European Standards do exist for such products, for example EN50131 series standards for intrusion and hold-up alarm system components; EN50132 series standards for CCTV systems and components; EN50133 series standards for access control systems and components.

Comments and assumptions

For the purpose of the assessment of the impacts of Option A it is assumed that:

- Appropriate harmonised European Standards are developed following the principles of stakeholder involvement and a consensual approach. It can be noted, however, that normal processes for creating harmonised standards can be time consuming. This may be an issue of substantial concern, particularly with regard to rapidly evolving technologies and in the context of security, changing threat scenarios. Accordingly, it may be appropriate to consider 'fast-track' options involving relevant stakeholders (including industry and user groups); for example by a panel of recognised public-private experts. Similar processes already exist, for example 'CEN workshop agreements';
- Appropriate harmonised European Standards (EN) are agreed upon; implying that national standards institutions approve these standards and (where they exist) withdraw their national standards. This presupposes that the definitions of European Standards are such that they can accommodate legitimate difference in security performance requirements that may be warranted, for example, as a result of differences in national, sectoral or activity-related (security) performance requirements;
- The scope of harmonised European Standards (EN) is such that they are sufficient to not only describe necessary performance requirements but also other aspects (e.g. supporting services such as planning and installation, interoperability, operational and integration requirements) that may otherwise provide a justification for (additional) national-level conformity assessment and certification requirements of security products or categories thereof. This does not preclude possible '*local*' approval/verification of installed security equipment and systems that may be normally required, taking account of the specificities of the environment (e.g. location or sector) in which the security product is employed;
- The necessary harmonised European Standards are also developed with respect to the conformity assessment procedures and methodologies, including test criteria etc., where relevant.

Organisation

The central element of this approach is the creation of a 'one-stop' EU-wide scheme for conformity assessment and certification. This presumes the existence of the necessary European Standards (as described above), enabling validation (testing) and certification of security products against agreed European (EU) requirements and specifications.

Currently various national structures exist for conformity assessment and certification of security products and in limited cases pan-European and industry-led schemes. The intention of this approach would be to bring such schemes under a single 'umbrella' for different security product categories, thus providing for a common (harmonised) EU-wide approach for conformity assessment and certification. This would not imply radical changes to existing structures for CAC (i.e. conformity assessment bodies / testing facilities and certification organisations) but would bring them under a common EU systems and procedures for approval (accreditation) of conformity assessment (and certification) bodies. This may, however, result in the exclusion of some existing conformity assessment bodies that do not meet the requirements for accreditation under the EU-wide approach[223]. On the other hand, it may be the case that the opportunities offered by the possibility to provide conformity assessment services and EU-wide recognised certification of security products will provide an incentive for new providers to enter the market.

[223] Where several conformity assessment bodies operate within a national or sector schemes for certification, it may be the case that only some of the bodies will meet EU requirements for accreditation. For example, several laboratories may be nationally accredited under existing schemes to provided conformity assessment (testing) services but not all of them may meet the (new) EU requirements for accreditation.

The CAC systems and procedures could be based on the existing 'generic' principles of EU conformity assessment (as set out under the New Legislative Framework (NLF); see Chapter 1. This would enable conformity assessment (e.g. product testing, inspection) to be undertaken within existing structures, maintaining the principle of independence of conformity assessment bodies (CABs), and following the arrangements for accreditation of CABs set out in the NLF.

Certification of products meeting European Standards may be provided by either of the following[224]:

- A National Certification Body (NCB), subject to mutual recognition by Member States of certificates issued by an appropriately accredited NCB in another Member State;
- A Sector Certification Body (SCB), operating an approved sector scheme, subject to recognition throughout Member States of certificates issued by the SCB.

Comments and assumptions

For the purpose of the assessment of the impacts of this kind of approach it is assumed that certification of security products is *a priori* 'voluntary'. Thus we draw a distinction between certification of security products and (mandatory) 'generic' conformity requirements for the placing of products on the EU market (i.e. CE label). This does not preclude the possibility that EU legislation may be implemented that would make compliance with EU minimum requirements mandatory (e.g. as is the case for fire systems under the Construction Products Directive/Regulation). In this respect, CE marking provides only an indicator that a product meets minimum EU requirements which, in itself, is considered insufficient to inform purchasers of security equipment (and other relevant stakeholders) on relevant security performance (and other) characteristics. Accordingly, it assumed that a distinct certification of security products will be required.

10.4.2 EU CAC for 'priority and sensitive' security products (Type-2)

Product coverage

The aim of this approach is to provide an EU-wide CAC system for security products employed as part of counter terrorism measures or in response to other identified EU priority security threats. It would be intended to provide a common system for testing, validating and certifying compliance with EU requirements for the performance of such security products. In comparison with a CAC system for general security products (Type-1), this approach would cover security products whose use is either required by EU security-related legislation or is in accordance with efforts to address security threats and challenges identified within the EU's Internal Security Strategy. Accordingly the products covered by the system should reflect EU security priorities and competences.

The scope of products covered by the system would give priority to newly developed technologies that address newly arising security threats or introduce new approaches for addressing security threats (e.g. automation of security functions such as passport/border controls). In this respect, the system would not be intended to cover those products already covered by an existing EU-level (or other widely accepted) CAC system providing testing, validation and certification of security performance. Moreover, it would not be the purpose of the system to cover products that could readily be brought within the scope of an existing EU-level (or other widely accepted) CAC system.

[224] We make the distinction between certification bodies and conformity assessment bodies, since testing laboratories and other conformity assessment organisations (e.g. inspection bodies) may not be accredited to (directly) provide certification services. In fact, these different categories of organisations are subject to different international standards for accreditation, for example: testing laboratories: ISO/IEC 17025:2005; inspection bodies: ISO/IEC 17020:1998; certification bodies: ISO/IEC 17021 (Management Systems), ISO/IEC Guide 65:1996 (Product Certification), and ISO/IEC 17024:2003 (Personnel Certification).

In terms of identifying the categories of security products that might be coved by a specific EU CAC system for security products, additional characteristics that might support inclusion of a product category may include, for example:

- The security performance requirements and associated test criteria relating to the product are 'sensitive' (e.g. classified or secret) information, requiring internal protocols for information confidentiality that are not available within an existing CAC system;
- The deployment of the product is immediately or imminently required (for example, in response to the evolution of security (terrorism) threats), requiring rapid ('fast-track') procedures that are not available within an existing CAC system.

Regulatory approach

For Type 2 security products, only for limited categories of products does existing legislation set out (essential and/or technical) requirements and corresponding conformity assessment and approval/certification procedures.

Comments and assumptions

In order to provide a baseline for assessing the impacts of EU policy options for conformity assessment and approval/certification of Type-2 products it is assumed that an appropriate 'legislative package' is implemented. This would include, as required, primary legislation (including essential requirements), implementation of legislation providing a basis for detailed technical requirements, as well as conformity assessment and certification system and procedures. It Is assumed, therefore, that as part of this kind of approach the following are implemented:

- **Primary legislation** setting out 'essential requirements' for security, compliance with which would need to be demonstrated. These requirements may be specified at the level of sectors or activities (e.g. aviation/airports, maritime/ports, etc.) or in relation to categories of security products and/or technologies;
- **Implementing legislation** setting out the technical specifications/parameters against which product coming within the scope of primary legislation (above) should be assessed in order to demonstrate conformity with essential requirements (and, where appropriate, the specification of test criteria etc.). Note: these specifications may:
  - be included directly in the implementing legislation;
  - make reference to European Standards (or other recognised international standards); where such standards do not exist but are considered to be the appropriate means of specifying technical specifications/parameters then the EC could issue a mandate to the ESOs (CEN, CENELEC, ETSI) to develop the required standards;
  - make reference to 'standards' of a competent organisation to define necessary technical specifications (e.g. ECAC for airport security equipment).
- **EU CAC/approvals system**, adequate to ensure compliance with the essential requirements and technical specifications set out in EU legislation, such a system and its procedures should be aligned between all Member States.

Organisation

Taking account of the general absence of existing EU-level structures and processes for defining and implementing conformity assessment and certification requirements and procedures for Type-2 security products, this sub-section attempts to indicate and outline the possible components of a such a structure.

Security Committee

This would constitute the strategic body responsible for identifying security capability requirements and corresponding product needs (and associated priorities for CAC). Its main responsibilities – based upon a common EU threat assessment – would include:

- Systematic foresight and monitoring process to identify upcoming 'discontinuous' security challenges and potential developments in security approaches/processes and technologies;
- Prioritisation of the categories of security products for which EU CAC procedures should be developed;
- Defining the capability needs and primary (fundamental) technical performance requirements for each (prioritised) category of security products;
- Determining if legislative measures are required to support (or make mandatory) the use of the EU system for CAC;
- The above activities could be supported through the establishment of sector committees or working groups for specific categories of security products or technology areas.

Comments:

- The Committee would need to include representatives of Member States administrations, together with relevant EU institutions. Consultation with Member States should serve to ensure that there is common agreement on the scope and priorities for the product categories covered by the system. This implies that the Committee should be able to establish a common EU threat assessment that integrates differences in national situations. In this regard, an observation that has been made – but which it is not possible to verify – is that with respect to ECAC (which has a broad participation of countries that are not all EU Member States), some countries are disinclined to share information on national threat assessments because they are concerned about the possible 'leakage' of information;
- It may be necessary to recognise that in some areas Member States may consider that, irrespective of the reliability and integrity of an EU-wide CAC system, they nonetheless have an essential obligation to undertake their own national testing and validation of certain categories of security products;
- By developing a strategic view of capability and technology requirements and priorities (as opposed to reacting to short-run changes in threat assessments) future needs for conformity assessment and certification should be identified. This, in turn, should provide a framework for linking together technology development requirements, on the one hand, and the preparation of infrastructure (including relevant specifications/standards and testing/validation capabilities) for approval/certification on the other. This should enable a more coordinated approach and faster implementation of testing, validation and approval/certification as new security products seek to enter the market.

EU Body for Security CAC

This would constitute the body responsible for oversight and coordination of the CAC system. In this regard, the following key roles would be fulfilled by the Body:

- to ensure that testing, validation and approval of security products is undertaken by qualified and independent organisations;
- to ensure that conformity to EU requirements is undertaken on the basis of objectively determined specification of common performance requirements, and common testing/validation criteria and procedures.

With respect to the first role, the Body would be responsible for[225]:

- EU approval (EU accreditation) of nationally approved (nationally accredited) testing laboratories to provide EU conformity assessment of security products;
- EU approval (EU accreditation) of nationally approved (nationally accredited) approval/certifying bodies to provide EU approval/certification of security products;
- Allocate individual products to EU approved laboratories for testing/validation;
- The above activities could be conducted in consultation with national authorities and/or the Security Committee.

With respect to the second role, the Body's main responsibilities would include:

- Setting detailed EU technical performance requirements (critical technical parameters) for individual categories of security products (and sub-categories, where relevant);
- Integrate, where relevant, other product requirements (i.e. not related specifically to security performance of products) to be also included in the scope of conformity assessment requirements;
- Specification of appropriate testing methodologies and test criteria;
- Setting procedures for verification of testing procedures (e.g. counter-testing of products, peer review).

The above activities could be supported through the establishment of (ad hoc) Technical Expert Groups.

EU Stakeholder Consultation Group on Security Standards and CAC

The Consultation Group(s) would provide a formal process to integrate manufacturers/ suppliers, procurers/users and other relevant stakeholders into the CAC system. Recognising the diversity of products/technologies and end-users (both private and public), the Consultation Group should be able to provide technical expertise and knowledge of operational and other requirements that may serve as inputs into the definition of common test criteria.

EU Accredited Security Testing Laboratories

These would be EU approved (accredited) testing laboratories for security products. They would provide independent testing of security products according to the approved test methodologies and test criteria determined by the Body for Security CAC.

EU Accredited Security Certification Bodies

These would be EU approved (accredited) certification bodies for security products. They would evaluate test results provided by the testing laboratories and approve products tested as conforming to EU technical performance requirements. They would issue certificates of conformity to EU technical performance requirements.

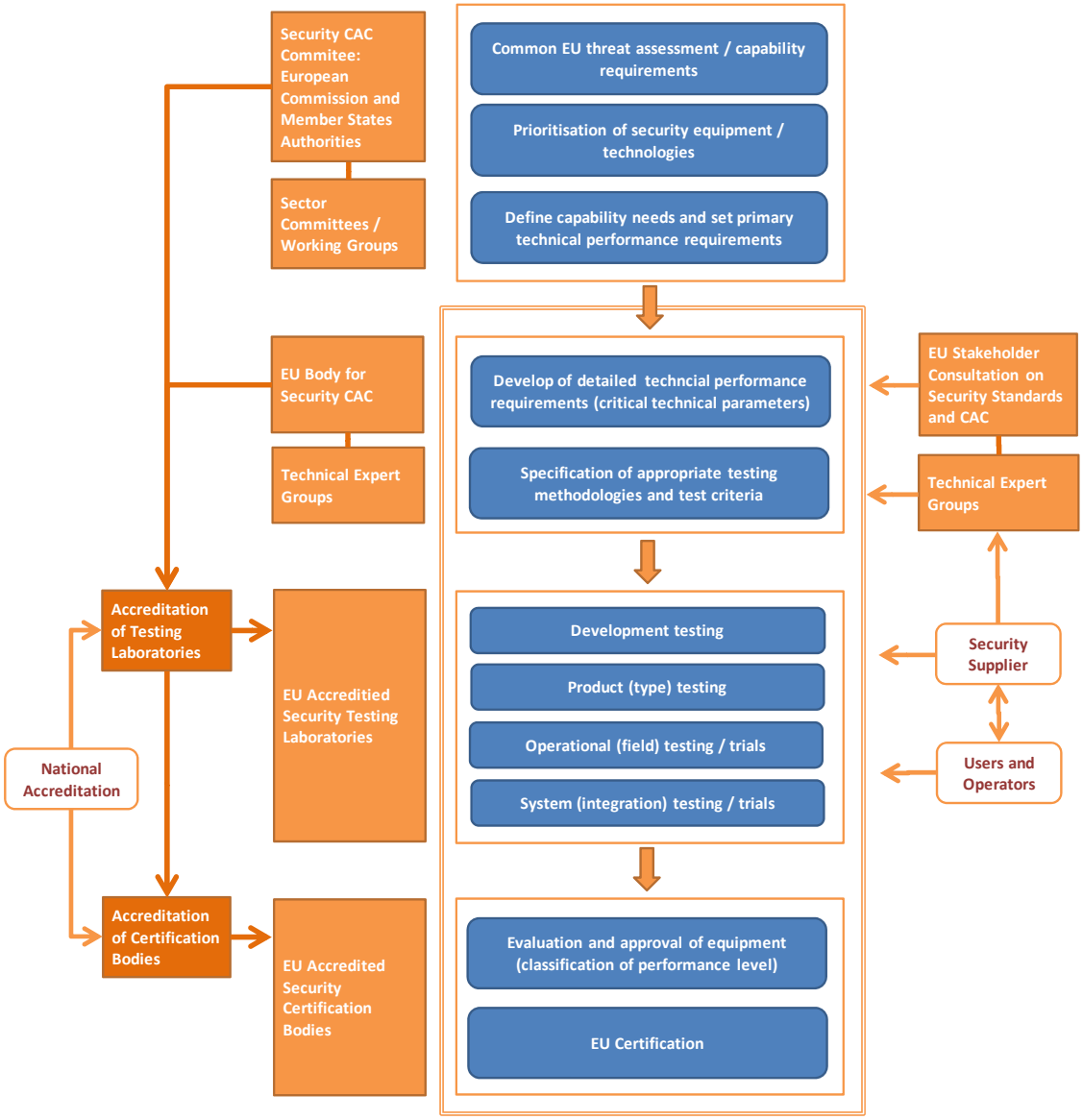
Comments:

- Certification could be undertaken by the relevant national authorities, with the provision that national approval/certification should be subject to mutual recognition. Such a possibility is provided for with respect to equipment for the screening of LAGs (liquids, aerosols and gels) under EU Regulation

[225] We make the distinction between certification bodies and conformity assessment bodies (e.g. laboratories), since testing laboratories and other conformity assessment organisations (e.g. inspection bodies) may not be accredited to (directly) provide certification services. In the case of Type-2 products it may, for example, be the case that testing activities are undertaken by independent testing laboratories but final approval/certification is made by the relevant national authorities. See, also, footnote 224.

185/2010[226]; although it is not certain how this will operate should a Member State raise an objection to an approval/certificate issued by another Member State. Alternatively, a more centralised approach could be adopted with approval/certification being issued by a single organisation; possibly the Body for Security CAC.

Figure 10.1 Organisation overview: CAC for Type-2 security products



10.4.3 Definition of policy options

The above has described the different approaches for an EU CAC scheme. The above did not address the choices for implementing these approaches that decision makers have, which are the policy options. Based on the terms of reference for this study, consultation of stakeholders and interaction with the European Commission, the following policy options have been identified:

[226] § 12.7.3 states that "*Equipment that is approved by or on behalf of the appropriate authority of a Member State to meet the standards as laid down in a separate Commission Decision shall be recognised by other Member States to meet these standards. Member States shall submit to the Commission the name and, upon request, other relevant details of bodies designated to approve equipment. The Commission shall inform other Member States of the bodies*".

- **Option 1 - Baseline.** This scenario represents a continuation of the currently existing situation. Here, no common EU-wide system providing conformity assessment and certification (CAC) of security products would exist. In the absence of mutual recognition, security products would need to undergo testing, validation and approval/certification procedures in each Member State where suppliers of security products wish to make their product available. No priority would be given to certain products. Furthermore, no EU-level structures and processes for the implementation of conformity assessment and certification requirements and procedures would exist;
- **Option 2 - A step by step approach.** This option would apply to the two types of products that are described in Section 10.3 (i.e. Type 1 and Type 2) and which would lead to two sub-components of this policy option:
  - ***Option 2.1*** *- EU CAC for 'general purpose' security products (Type-1).* Intended to cover security products aimed towards 'general' security markets and/or based on comparatively mature technologies (Type-1);
  - ***Option 2.2*** *- EU CAC for 'priority and sensitive' security products (Type-2).* Intended to cover security products aimed either towards 'specific' markets and/or based on comparatively new or innovative technologies (Type-2).
- **Option 3 – An all-encompassing approach.** This would be a situation where an EU-wide CAC system is in place for all security products (hence type-1 and type-2) all at once. No staging between product types is foreseen.

These options are subject of the impact assessment in the next chapter.

10.5 Prioritisation of security products and technologies to be covered by an EU-wide CAC scheme

The preceding sections outlined two approaches for developing EU-wide CAC schemes for different types of security products. As noted, however, there is a wide diversity of product categories and technologies that may fall within the scope of a possible EU-wide CAC scheme. Accordingly, in this section some of the possible criteria that may be utilised for prioritising products and technologies to be covered are discussed.

As a starting point, it is worth recalling that three main policy challenges have been identified (see Section 10.3.2) that may, in turn, provided appropriate criteria for prioritising security products and technologies:

- **EU Internal Security:** from a security perspective the overriding concern is to ensure the rapid and effective deployment of security products/technologies to ***address the most pressing security threats and challenges***. This requires linking information on security threat assessments and scenarios to capability requirements and corresponding security product/ technology development and deployment. Evidently, detailed information on current threat assessments is not in the public domain, thus making it difficult within this Report to identify those products and technologies that would be priorities from the perspective of EU Internal Security. In a slightly more general context, the work undertaken by ESRIF provides, for example, some indications of priority areas for technology development and innovation in the area of security. Taking into account on-going developments in these priority areas (i.e. closeness to actual deployment of 'new' solutions) this may provide a basis for identifying and prioritising those products and technologies for which standards and CAC schemes may be most imminently required. This would suggest the need for an on-going 'technology watch' to monitor security technology developments and innovations. A link may also be made to public funding programmes (e.g. EU Framework Programmes and Member State's research and

innovation support), perhaps to the extent of including consideration of possible CAC requirements within the scope of projects;

- **EU Internal Market:** from an internal market perspective the main consideration is to reduce the existing fragmentation of markets within the EU. Accordingly, the main criteria for prioritisation of security products and technologies to be covered by an EU-wide CAC scheme would relate to the ***prevalence and magnitude of barriers to trade*** and to the extent to which there is a lack of a 'level playing field' within the EU;
- **EU Industrial Policy:** from an industrial policy perspective, two criteria for prioritising products and technologies to be covered by an EU-wide CAC scheme come to the fore. Firstly, the potential to ***reduce costs and administrative burden*** placed on manufacturers/suppliers of security products as a result of existing CAC requirements (e.g. multiple certifications). Second, the potential contribution that an EU-wide scheme could make to enhance the competitiveness of the EU security industry. Concerning this second criterion, two particular elements may be identified. On the one hand, the benefit to the EU security industry can be expected to be greater for those product categories and technologies where ***EU industry has a comparatively strong market position*** and for which a more unified market within the EU could serve to reinforce this position (e.g. strong 'home' market as a support for international/global competitiveness). On the other hand, are the potential benefits that may come from developing EU-wide CAC schemes that also ***support technology development and innovation*** by EU industry, particularly in those areas where market opportunities (both within the EU and globally) are expected to be strongest.

The above discussion highlights certain criteria that may be used to identify priority security products and technologies starting from a policy-area based approach. To these, may be added some more practical and pragmatic considerations that may influence the prioritisation of products/technologies to be covered by an EU-wide CAC scheme:

- **Speed and ease of implementation:** an EU-wide CAC scheme may be more quickly implemented and show effective results if it is able to build upon existing CAC infrastructures and where recognised standards already exist or can easily be developed. In the case of Type 1 products, for example, some schemes for pan-European certification already exist (e.g. CertAlarm) that could provide the basis or template for an EU-wide CAC scheme. Also, European Standards (EN) have already been established for some products and components. Accordingly, an EU-wide CAC scheme may be relatively easily introduced and could be expected to have a rapid impact on the sector/market;
- **Long term benefits for industry, customers and citizens:** developing an EU-wide CAC scheme for products and technologies addressing many 'priority' security challenges may require more time to implement and to demonstrate its effectiveness but may yield greater 'benefits' in the longer term. In the case of Type 2 products, for example, it is typically the case that recognised standards do not exist and that existing CAC infrastructures are relatively limited. Moreover, Type 2 products covers more complex equipment and larger security systems the deployment and operation of which is often specific to a particular environment/context. This may require approaches for CAC that are not based on individual products (i.e. no "one fit for all" approach) but may necessitate inspection-based or audit-based approaches based on 'guidelines' for integrated systems as opposed to defined technical requirements and standards.

The relative weight that may be attributed to the above 'considerations' is to a large extent a 'political choice' that is beyond the scope of this Report to determine.

Although as part of the study various stakeholders have been consulted as to which specific security products and technologies can be identified as priorities for possible EU-level policy intervention, opinions on the issue are limited and without any general consensus:

- **For Type 1 products**, a starting point may be to start with security alarm and hold-up alarm systems (for which there is already a private/industry led scheme; CertAlarm) that may be extended to other categories of security electronics products for which European Standards exist (e.g. sensors, control panels) and towards other forms of perimeter and surveillance equipment (e.g. security CCTV systems);
- **For Type 2 products**, a similar approach of building on existing schemes/procedures would bring in products where EU performance requirements already exist (e.g. airport scanners, biometric identity documents). In the case of scanners, this may be extended towards cargo and container scanners which would be relevant for both the aviation and maritime sectors and would have wider application in terms of supply chain security in general. Another area that has been mentioned is eGate type solutions for border control management, which could also have possible applications beyond the aviation sector. However, it remains uncertain at this time as to whether there will be wider deployment of eGate type solutions in the future and, therefore, whether a specific EU CAC scheme would be worthwhile. However, a broader based EU CAC scheme could be considered that would cover biometric based access control systems employed in a variety of security context.

In general, the limited identification of priority products / technologies suggests that there remains a need for greater monitoring of EU markets for security products and of developments in security products and technologies. It may be appropriate therefore for the European Commission to set up or support a monitoring scheme/methodology, which could include also consultation with stakeholders representing both the supply and demand side and authorities with security responsibilities. This could serve to identify those areas where standards and CAC requirements are most pressing.

11 Impact assessment of policy options for conformity assessment and certification of security products

11.1 Introduction

This chapter provides an assessment of the impacts of the two policy options that have been described in the previous chapter. The approach that has been applied follows the logic and guidance of the Guidelines for Impact Assessment of the Commission.

The nature and character of the security sector has proved to be a strong limiting factor for the quantification of the impacts, and sometimes even in qualification of the proposed policy options. From both the supply-side and demand-side there is hesitancy to provide information that may be deemed sensitive from a security perspective. Furthermore, information may also be commercially sensitive in so far as it relates, for example, to the cost structures of suppliers of security products. It should also be noted that costs associated to conformity assessment procedures (e.g. fees for product testing) are typically negotiated between the product supplier and providers of conformity assessment services. Unfortunately, the aforementioned limitations also hamper any distinction in the assessment of impacts between different segments of the security sector/market under study in this project (aviation, maritime etc.).

Following from the above, the present assessment has largely been based on information obtained from stakeholder interviews conducted for the country case studies, position papers of the industry on the topic, and causal chain analysis based on the problem assessment regarding the conformity assessment and certification of security products as described in chapter 9. In line with the Commission's Guidelines for impact assessment, the economic impacts and social impacts are addressed. In the impact assessment below, economic impacts are market with an **{E}** and social impacts with an **{S}**. The Guidelines also indicate that environmental impacts should be assessed. However, the environmental impacts have not been assessed as they are considered to be minimal and of limited relevance in the context of the study.

Summary of analytical baseline

Key in any impact assessment is that the policy options are compared with a baseline situation; essentially the baseline option reflects the current situation and assumes no significant (new) policy intervention. The impact of the policy option is assessed relative to the baseline option. For the purposes of the analysis of impacts the baseline is characterised as follows:

- **Type-1:** This reflects the current situation where there is national conformity assessment and certification for some Type-1 products only. While, the remainder of the Type-1 products do not fall under any national conformity assessment and certification system. In the baseline option there is no mutual recognition of certificates;
- **Type-2:** This reflects the current situation where existing legislation sets out (essential and/or technical) requirements for only limited categories of Type-2 products. For these products, *ad hoc* systems and procedures exist for the corresponding conformity assessment and approval/certification procedures necessary to demonstrate compliance with legislation. There is, however, no EU-level scheme – with corresponding structures and processes – for systematically defining and implementing conformity assessment and certification requirements and procedures for Type-2 security products.

11.2 Assessment of impacts of Option 1 (baseline)

Key in any impact assessment is that the policy options are compared with a baseline situation; essentially the baseline option reflects the current situation and assumes no significant (new) policy intervention. The impact of the policy option is assessed relative to the baseline option. For the purposes of the analysis of impacts the baseline is characterised as follows:

- **Type-1:** This reflects the current situation where there is national conformity assessment and certification for some Type-1 products only. While, the remainder of the Type-1 products do not fall under any national conformity assessment and certification system. In the baseline option there is no mutual recognition of certificates;
- **Type-2:** This reflects the current situation where existing legislation sets out (essential and/or technical) requirements for only limited categories of Type-2 products. For these products, *ad hoc* systems and procedures exist for the corresponding conformity assessment and approval/certification procedures necessary to demonstrate compliance with legislation. There is, however, no EU-level scheme – with corresponding structures and processes – for systematically defining and implementing conformity assessment and certification requirements and procedures for Type-2 security products.

There is hardly any information available of the existing volume of CAC procedures in Europe. As an indication we provide the number of certifications for security products in aviation from two sources in the table below. These are essentially type-2 products. As the table suggest, the annual number of certifications may differ substantially per year.

Table 11.1 Number of annual certifications for aviation security products

	ECAC*	STAC**
2005		6
2006		1
2007		4
2008		14
2009		18
2010	14	3
2011	14	1
Total certifications	**28**	**47**

* https://www.ecac-ceac.org/activities/security/cip_for_security_equipment.
** DGAC France, Service Technique de l'aviation civile: http://www.stac.aviation-civile.gouv.fr/surete/tablocertimat.php.

In the remainder of this section the impacts of the 'do nothing' baseline scenario are discussed. These are mainly a presentation of identified problems, negative consequences and improvement areas of the current situation, as have extensively been described in the previous chapters. These are discussed for the following five stakeholder groups, which will also form the outline for the assessment of impacts of the options 2 and 3 in the Sections 11.3, 11.4 and11.5:

- Producers;
- Procurers / users;
- Conformity assessment and certification bodies;
- Regulators;
- Society.

11.2.1 Impacts for producers/ suppliers

Impacts associated with CAC requirements

The main identified impacts related to the CAC requirements in the current situation are:

- Costs of complying with multiple national procedures;
- Delay in 'time to market' of products;
- Adaptation costs to meet national conformity assessment and certification procedures and standards;
- Slow development and diffusion of new security technologies and solutions.

Costs of complying with multiple national procedures {E}

In a situation where no EU-wide system of conformity assessment and certification (or mutual recognition of such procedures) exists, security products will have to be certified once for each country where they are introduced. The costs involved in undergoing multiple conformity assessment (testing) and certification procedures can be substantial. In section 11.3.1 an illustration of the costs involved in conformity assessment and certification is provided. In the same section it is also claimed that SMEs are affected more heavily by these cost inefficiencies than larger companies, due to the fact that the costs for CAC procedures per product are the same, but the number of products sold is usually lower for SMEs.

Delay in 'time to market' of products {E}

The requirement of obtaining multiple national certifications causes delays in the introduction of products in the European market. Producers are not able to rapidly enter the entire European market (or a number of EU Member State markets) and are forced to delay or even refrain from product launches due to the requirement to undergo multiple conformity assessment and certification procedures. As a consequence, the scale of production cannot be aligned with the expected EU-wide sales volumes. Also, competitors are able to copy innovative products once they have been introduced on one market, reducing the competitive benefit for the producer that invented the product.

Adaptation costs to meet national conformity assessment and certification procedures and standards {E}

Producers can be required to produce several variants of products for different markets due to different product standards and conformity assessment and certification procedures throughout the EU. This implies additional production costs for manufacturers than if a single variant could be used to supply across the EU.

Slow development and diffusion of new security technologies and solutions

Reduced market access may act to inhibit the development and diffusion of new security technologies and solutions, while undermining the competitive position of EU suppliers. For example, EU companies that develop new technologies to address new threats suffer in comparison to competitors, in particular from the U.S., if their equipment is not as quickly tested, certified and installed as their competitors.

Impacts on market conditions

The main impacts on market conditions are:

- A lack of transparency on product performance {E};
- Market fragmentation {E}.

Lack of transparency on product performance {E}

The absence of an EU-wide CAC scheme and mutual recognition of conformity assessment and certification procedures means there is also no EU-wide, recognisable objective indicator that a

product meets certain standards or is of certain quality. The existing differences in national product and conformity assessment standards underlying national CAC procedures result in uncertainty and a lack of transparency over product performance. This hampers in particular smaller companies who are less well known on the market.

Market fragmentation {E}

As indicated in Chapter 1, the situation with national CAC procedures leads to a lack of market transparency and openness. As a result the market for security products is fragmented. The Consultation on an Industrial Policy for the Security Industry carried out by the European Commission indicated that stakeholders observe clear problems in market conditions. The consultation shows that more than 80 percent of the responding firms agree that the lack of harmonised conformity assessment and certification procedures is associated to market fragmentation.

11.2.2 Impacts for procurers/ users

For procurers, the following effects of the existing situation are identified:

- Lack of transparency *{E}*;
- Limited choice of suppliers *{E}*.

In line with what was indicated in the previous section, procurers of security products also experience a lack of transparency with regard to the quality of products. As a result, they often limit their scope to the suppliers with whom they are working already, but who may not always be the most beneficial supplier in terms of product performance, price, etc. Also their choice of products is limited because some foreign producers may not serve the national market, for the reasons explained in the previous section 11.2.1.

11.2.3 Impacts for conformity assessment and certification bodies and system

In the existing situation, CAC bodies in the area of security are limited and have a near monopoly position in the Member State where they are based. This position is maintained due to the fact that suppliers of security products are obliged to have their products certified in each Member State and cannot opt to have their product certified once for the entire EU.

11.2.4 Impacts for regulators

Regulatory bodies of countries that have a well-functioning infrastructure for developing relevant product/security standards and verifying the conformity of security products in place will not see an immediate need to introduce an EU-wide CAC scheme. Some countries, however, lack the technical expertise and capacity to support such functions. This may limit the scope for developing and implementing regulations requiring conformity assessment of security products and may result in insufficient or appropriate national regulatory frameworks for security products. Such circumstances may necessitate that Member States make reference to, and are reliant upon standards to certification procedures available from other Member States but which may not be aligned to their own national situations.

11.2.5 Impact for society

Following from the sections above, it is clear that in the current situation inefficiencies with regard to the certification of security products exist. Due to the existence of multiple national requirements, the functioning of the European market for security products is hampered. Products cannot be

supplied to all EU countries, or can only be supplied with delays. As a result, users of security products are not always able to buy the best security products at the lowest price. Also, in countries where no infrastructure can be put in place to establish and verify compliance with required performance standard of security products, products falling below minimum requirements can be placed on the market.

Development of standards and procedures for testing, approving and certifying new equipment (and new technologies) that are developed – and required – to respond to new security threats (e.g. body scanners) can be relatively slow, which may impact negatively on the overall security of citizens.

11.3 Assessment of impacts of Option 2.1 (Step-by-step approach for Type-1 products)

In this section the impacts of Option 2.1 are assessed: a step-by-step approach for introducing EU CAC for 'general purpose' security products (Type-1 products). These impacts are again described for five stakeholder types:

- Producers;
- Procurers / users;
- Conformity assessment and certification bodies;
- Regulators;
- Society.

11.3.1 Impacts for producers

Impacts associated with CAC requirements

The main identified impacts that relate to the CAC requirements as a result of Option 2.1 are as follows:

- Reduction of costs associated to multiple testing to obtain national certification;
- Increase of costs to obtain EU certification;
- Reduction of the 'time to market' of products;
- Reduction of costs associated to adaptation of products to meet different national standards and other technical specifications;
- Reduction of costs for CAC services.

These impacts are further elaborated below.

Reduction of costs associated to multiple testing to obtain national certification {E}

Under an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU, security products will have to be certified only once, instead of multiple times. This implies a reduction of costs associated to multiple conformity assessment (i.e. testing) and certification for those products, and in those markets, that are currently required to undergo national conformity assessment and certification.

Illustration: Conformity assessment and certification of alarm systems.

Currently a producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States. The costs of certification of an

alarm system are on average (with a large spread depending on the nature of the product)[227] at the level of EUR 200-300 thousand for full access to Europe including all tests. With the introduction of one common CAC scheme with mutual recognition of the certificate across the Member States, these costs of conformity assessment and certification should be reduce significantly. Stakeholders indicate that the estimated cost for obtaining a mutually recognised certificate for the same alarm system would amount to EUR 40-60k. Compared to the current national schemes, the total savings for a single Type-1 product from a common EU scheme for conformity assessment and certification would amount to a figure in the region of EUR 160-240k.

Information obtained from industry sources in France indicate that the annual total direct costs (covering initial laboratory tests, factory process control and certification fees) to manufacturers for certification of intruder alarm systems (NF & A2P certification) is in the region of € 450 to € 500 thousand[228]. This, however, does not include preparatory costs or additional costs that may associated with product adaptations etc. required to meet different national approval/certification requirements, which are thought to double overall costs for manufacturers.

Quantification: The costs of certification and conformity assessment for producers in Europe: the case of intruder alarms

Based on the industry estimate as described above, the direct costs for certification have been estimated for France to be around EUR 500 thousand per year. This is the direct cost for certification, and the estimate is that the company costs in preparation for multiple listings and in different product specifications for the different approval needs could well cost this amount again. Hence total costs for certification and conformity assessment for intruder alarm systems are in the order of magnitude of EUR 1 million per year for France.

Our estimate of the total market for intruder alarm systems is around EUR 1.1 billion in 2010. However, there is no information available how this is distributed over member states. It is assumed therefore that this value for France as indicated above is replicated across Europe and is roughly in line with the GDP. Given a share of France of 16% of EU economy, then this would suggest a total cost for producers in Europe of around EUR 6.2 million per year for certification and conformity assessment of intruder alarms.

Estimates from other sectors, suggest that the cost associated to differences in technical rules and multiple testing/certification are between 2% to 10% of production costs[229]. This is an estimate for different products outside the security sector, and has been applied in the Commission's impact assessment for the New Legislative Framework[230]. The same impact assessment indicates that in 2002 43% of enterprises in the area of burglar alarm systems have encountered problems with mutual recognition. From these sources it is unclear what costs are precisely included in the range of 2%-10%. Therefore, in order to be conservative, the lower bound of the estimate is taken for this study of 2% of production costs. It is also not clear what proportion of the total market of intruder alarm systems of EUR 1.1 billion is covered by products/systems that require certification. If one assumes that 75% of the market is covered by certified products, this would

---

227 CAC costs vary significantly depending on the type of product and specific characteristics. There are also differences across countries in the fees charged for CAC.

228 This figure relates to (voluntary) certification NF & A2P. For more information on NF & AP2 certification see the joint AFNOR-CNPP document "Certification rules Electronic Security Equipment: Intrusion Detection, Access Control Management Systems" available at: http://www.cnpp.com/fr/Mediatheque/Autres-documents/Certifier-image/H58/REFERENTIEL-NF324-H58-VERSION-ANGLAISE-OCTOBRE-2010.

229 Fabienne Ilzkovitz, Adriaan Dierx, Viktoria Kovacs and Nuno Sousa, « Steps towards a deeper economic integration: the internal market in the 21st century", European Economy, Economic Papers, No. 271. January 2007. European Commission.

230 European Commission, 2007, Impact assessment on Directive laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision 3052/95/EC, SEC(2007) 112/2.

give a market value of EUR 825 million. At 2%, this would suggest a cost to the industry of EUR 13.2 million, where production costs have been taken at 80% of the total relevant market value of EUR 825 million.

The total costs for certification and conformity assessment of intruder alarm systems is thus estimated to range between EUR 6.2 million and EUR 13.2 million per year. These costs cannot be reduced completely under this policy option. After all, there is still need for a single certification and conformity assessment, and associated need for testing etc. It is assumed that a single EU system of reduces the cost associated to differences in technical rules and multiple testing/certification by three-quarters (75%). This would suggest a saving of EUR 4.7 million to EUR 9.9 million per year.

SME versus large producer cost impacts

Assuming that costs for undergoing conformity assessment (testing) and certification are broadly equal for similar products within a particular product category, the cost of CAC as a proportion of total costs (production and marketing costs) will be inversely proportional to the volume of production/sales. As SMEs a more likely to produce/supply individual products in small volumes, the share of CAC costs in total costs will be higher than for larger producers with higher volumes of production/sales. Moreover, SMEs having more limited financial resources may find it more difficult to cover the 'upfront' costs of undergoing conformity assessment and certification necessary to supply to a particular market. Accordingly, multiple CAC requirements are likely to impose a greater burden on SMEs than on larger-scale producers of security products. Conversely, the reduction of costs associated with moving to a 'one-stop' system with mutual recognition of certification will be greater (in proportional terms) for SMEs. Thus, even if in absoluter terms the cost saving for an individual product will be more or less equivalent for all producers and larger producers will benefit more in absoluter terms if they supply a larger number of individual products (broader product range), in relative terms the cost reduction – and hence competitiveness – impact of Option 1 can be expected to be greater for SMEs.

Additional costs of obtaining EU certification {E}

For products that are currently not covered by national conformity assessment and certification requirements but that will be brought within a future EU-wide system under Option 2.1, there may be an additional cost for obtaining certification. Even if certification is not made mandatory, there may still be a development towards a situation where the market requires products to be certified and, consequently, certification becomes a *de facto* obligation. Alternatively, based on a commercial decision, suppliers may voluntarily choose to obtain certification a means to provide an independent verification of the 'quality' of their product so as to distinguish them on the market.

SME versus large producer cost impacts

Conversely to the cost reduction associated with the removal of national CAC requirements, for products currently not covered by CAC requirements that would be brought within the scope of an EU-wide system, the (proportionate) additional cost impacts of Option 1 will be greater in relative terms for SMEs than for larger companies.

Reduction of the 'time to market' of products {E}

Under Option 2.1, having obtained a recognised EU-wide certificate, products may be introduced into all EU-markets without the delay caused by requirements to obtain national certification. This implies that suppliers are more rapidly able to (potentially) access the whole EU market rather than staggering product launches in accordance with time taken to undergo separate conformity assessment (testing) to obtain national level certification. This may have a number of implications for producers, for example:

- The scale of production can be aligned at the outset to the expected EU market as a whole rather than being conditioned on (uncertain) timing of national certification. This may result in more efficient investment and utilisation of production capacity and economies of scale;
- The risk that competitors are able to 'replicate' new product developments and innovations is reduced. As a new product can be introduced simultaneously throughout the EU market, this limits the possibility that delays resulting from CAC requirement provide competitors with the opportunity to develop and launch their own similar products. Consequently, the potential returns from investments in research and technology development (RTD) are increased.

Reduction of adaptation costs to meet national product standards/specifications {E}

Another way in which cost impacts occur is related to situations where divergent national product standards and specifications exist within the EU. Where this occurs, producers can be required to produce different variants of their products for different markets in order to meet national standards and specifications. This means, for example, that a manufacturer of a specific type of CCTV surveillance camera has to manufacture several variants of the same product so as to meet specific requirements set in national regulations in different Member States. Thus, instead of producing a single product, the producer must meet the additional cost (both in development and production) of adapting products to individual national markets. Introducing an EU-wide system of conformity assessment and certification, based on harmonised European product standards, should remove the need – and hence cost – for products to be adapted to meet differing national standards and specifications.

Reduction of adaptation costs to meet national conformity assessment procedures {E}

Linked to the previous item, it is evident that national conformity assessment procedures and corresponding testing criteria etc. reflect differences in national product standards and specifications. However, it has been indicated by some stakeholders that, notwithstanding differences in standards and specifications, differences in national testing procedures and protocols can also necessitate further adaptation of products. Introducing an EU-wide system of conformity assessment and certification, with common European protocols and testing criteria, should remove the need – and hence cost – for products to be adapted to meet differing national standards and specifications.

Reduction of costs of CAC services {E}

An EU-wide system of CAC that provides for mutual recognition of certification throughout the EU, would have the effect of opening up the market for CAC services within the EU to greater competition. This impact is elaborated in Section 11.3.3. For producers, the expected outcome can be a reduction in the prices and/or improvements in the quality of CAC services that they utilise.

Impacts on market conditions

The Consultation on an Industrial Policy for the Security Industry carried out by the European Commission indicates that stakeholders observe clear problems in market conditions. The consultation shows that more than 80 percent of the responding firms agree that the lack of harmonised conformity assessment and certification procedures is associated to market fragmentation. They also expect that an EU-wide CAC system will be an effective way of reducing this fragmentation. Interviews with stakeholders as part of the present study (including inputs for the national case studies) confirmed this view. Drawing on these inputs and the analysis of the present study a number of impacts related to market conditions have been identified and assessed:

- Certification as indicator of product performance;
- Minimum standards as *de facto* requirement;
- Increased competition;
- Increased competitiveness of European manufacturing industry.

These impacts are further elaborated below.

Certification as indicator of product performance {E}

Third-party product certification provides independent verification that a product meets the (performance) requirements against which it is certified and, hence, is an 'objective' indicator for product performance or 'quality'. In the case of products that are currently not covered by national conformity assessment and certification requirements, an EU-wide certification scheme enables a supplier to demonstrate to potential customers throughout the EU that its product meets EU performance requirements. In the case of products that are covered by national conformity assessment and certification requirements an EU-wide certification scheme would have a similar effect but may also reduce 'uncertainty' over product performance that can result from differences in the underlying national product and conformity assessment standards and specifications. In this regard, Option 2.1 provides for greater transparency of certification and, consequently, of product performance throughout the EU. Since products are certified as conforming to common EU-wide performance requirements, this should facilitate market acceptance of products being offered to the market by 'new' suppliers as it may reduce the importance of 'reputation effects' of established companies. Accordingly, it may be of particular importance for smaller companies (including new business start-ups) and to non-local suppliers that are less well known on the market. As such, certification can act to reduce market entry barriers.

Minimum standards as de facto requirement {E}

There exists an inherent risk that setting (minimum) product performance requirements and a corresponding system for conformity assessment and certification leads to a situation in which products certified as complying with the minimum standard becomes the *de facto* market requirement. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or innovative' products, particularly if they are more costly than standard products that comply with minimum requirements. Essentially, this is an issue that concerns the appropriateness of the standards underpinning the conformity assessment and certification system, irrespective of whether these are associated or not to an EU CAC procedure. However, a possible negative impact of an EU-wide system of CAC that provides for mutual recognition of certification throughout the EU is that it reduces the incentive to produce products with performance levels above the EU minimum standards/specifications.

Increased competition in security product markets {E}

Following from the discussion of different impacts on producers outlined above, there are two main mechanisms through which Option 2.1 will affect competition in the market for security products:

- First, a single EU-wide system of CAC with mutual recognition of certification should result in an increased in market *transparency*. Products will be certified against common European Standards, providing procurers and users with more insight on the relative performance characteristics of products;
- Secondly, a single EU-wide system of CAC with mutual recognition of certification should increase market *openness* (i.e. reduced market access barriers). An EU scheme allows products to be sold more easily to customers in multiple countries than in a system where products are subject to CAC procedures for each Member State.

Both of these mechanisms should reduce fragmentation and increase the level of competition within markets for security products. As noted, existing suppliers will be more easily able to serve different national markets and such effects may be particularly beneficial to SMEs. The EU market would also be more attractive to new entrants; both new business start-ups and non-EU based suppliers.

For the latter, a common EU-wide certification scheme may significantly reduce the entry barriers created through different national level CAC requirements. The extent to which non-European producers will seek to enter and/or increase their presence in the European market, will differ between submarkets but can be expected to be most important for more standardised products. Overall, under normal market conditions, increased competition will put downward pressure on the price of security products, which would reduce costs for procurers / users of the products.

Increased competitiveness of European manufacturing industry {E}

In terms of impacts on the competitiveness of European producers, the main identified mechanisms are as follows:

- Increased market openness and transparency should raise competition and within the EU market. Essentially, an EU-wide system of CAC with mutual recognition would reduce the extent of protection provided to incumbent suppliers as a result of existing differences in CAC requirements and systems. This increased competition should drive improvements in productivity performance by forcing improvements in production efficiency and/or raise value added (e.g. higher value-added products);
- Improved market access, which increases the size of the potential market for new products, should provide a positive incentive for producers to engage in RTD activities and promote innovation. Essentially, access to a wider market increases the potential returns from such development and innovation activities. Interviews with stakeholders confirmed that current market fragmentation is a major barrier to innovation;
- Finally, EU certification may support exports of products to markets outside the EU. A single EU certification may engender greater recognition in international markets than the existing multitude of national certification schemes. Thus, EU certification may be more widely recognised as an international 'quality label' and, hence, support the international competitiveness of European producers. It must be recognised however, that non-European producers that obtained the same European certification would benefit in an equal way from this 'quality label'.

11.3.2 Impacts for procurers / users

There are a number of impacts for procurers and users. As these form the demand side of the market, many of these impacts are related to the impacts as described above under producers. The following impacts have been identified:

- Lower price for security products;
- Increased product choice / availability;
- Enhanced information / transparency on product performance;
- Facilitation of procurement procedures;
- Reduced uncertainty of compliance with (user) security regulations.

These impacts are further elaborated below.

Lower price for security products {E}

The previous subsections outlined a number of impacts that affect producer costs and prices and that should feed through to the purchase cost of security products:

- First, there is a decrease in conformity assessment and certification costs. In a market with increased competition it may be anticipated that these costs savings are passed on to procurers /users;
- Secondly, increased market openness should promote production efficiencies and scale economies for producers. Again these should reduce costs and lower product prices;

- Thirdly, the increased competition will lead to price reductions as described above, at the benefit of the procurers / users.

Increased product choice / availability {E}

A second impact for procurers / users is the possible increase in product choice and availability. This stems from increased market openness, resulting in more suppliers on the market (European and non-European). At the same time, to the extent that a less fragmented EU market promotes RTD and innovation, there should be increased entry into the market of new technologies and innovative solutions.

Enhanced information / transparency on product performance {E}

An EU-wide conformity assessment and certification scheme should increase market transparency and provide potential purchasers with greater information on product performance. Overall, this should contribute to reducing information asymmetries between purchasers and producers. As described above, product certification provides an independent verification of product performance. As such, it provides purchases with additional insight into product performance.

Facilitation of procurement procedures {E}

Linked to the previous point, an EU-wide conformity assessment and certification scheme should facilitate procurement procedures. Procurers – and where relevant regulatory authorities – would be able to include EU standards and an EU certification as a requirement in their contracts. Furthermore, an EU wide scheme with mutual recognition of certification should support greater openness in procurement procedures by making it easier for potential suppliers to demonstrate conformity to EU standards/specifications rather than needing to undergo separate national procedures. This should increase the number of potential suppliers and result in lower prices of products, as argued above. A benefit related to this will be that the quality of tenders received will be better, as offers from suppliers that do not meet the minimum requirements (as represented by EU certification) will automatically be put aside. Interviews with stakeholders confirmed this to be an advantage of the EU certificates for the procurement of security products that they use. Finally, the procurement process for procurers with a presence in multiple European countries is improved. These procurers will now be able to procure security products for their entire pan-European company, as they different national certificates would no longer be required.

Reduced uncertainty of compliance with (user) security regulations {E}

As a final point, where procurers/users of security products are subject to regulatory requirements concerning their security arrangements but where these do not specify requirements for specific products/equipment, the utilisation of certified products may support their compliance with legislation. At least, employing products certified as complying with (EU) performance requirement may reduce uncertainty for users concerning the appropriateness of such products.

11.3.3 Impacts for conformity assessment and certification bodies and system

The following main impacts on conformity assessment and certification bodies have been identified:

- Change in the volume of demand for conformity assessment and certification services;
- Increased competition for the provision of conformity assessment and certification services.

Change in the volume of demand for CAC services {E}

By replacing multiple CAC requirements by a single ‘one-stop’ EU-wide approach, a clear consequence is that the total number of CAC procedures will decrease and, thus, turnover of conformity assessment and certification bodies will decrease; this is valid for products that are currently covered by national conformity assessment and certification requirements. Conversely, for

products that are currently not covered by national CAC requirements and that are brought within the scope of an EU-wide scheme, there will be an increase in the volume of demand for CAC procedures. Due to a shortage on data on current CAC volumes and the fact that demand under Option 2.1 will depend on the scope of a 'one-stop' EU-wide approach, it is not possible to assess the net effect of these two impacts. Nonetheless, it seems probable that an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU would result in a reduction in the overall demand for CAC services.

Increased competition for the provision of CAC services {E}

Interviews with stakeholders indicate that currently CAC bodies in the area of security often have a near monopoly position in their respective Member States; this is reflected in large differences across countries in the procedures and requirements of conformity assessment bodies (CABs) and certification bodies (CBs) and, also, in prices and average duration of CAC processes. The introduction of an EU-wide CAC scheme with mutual recognition of certification should remove the controlling position that CAC bodies are able to occupy over their national markets. Producers would have greater flexibility to choose the CAC bodies that they utilise to obtain certification, which should promote competition between CAC bodies. Increased competition may reduce the prices charged for such services and should also raise the 'quality' and professionalism of provided services.

Strengthened EU-wide accreditation {E}

It is foreseen that the anticipated organisation under Option 2.1 will includes EU accreditation of conformity assessment and certification bodies following common rules and requirements for obtaining accreditation. In this way, the independence and integrity of conformity assessment and certification bodies is maintained. There may also be some improvement in overall quality of services as a result of common requirements for accreditation.

Increase of administrative costs related to the CAC system {E}

It is foreseen that conformity assessment and certification bodies will be EU accredited, which will result in corresponding (additional) administrative costs. A detailed costs assessment is not feasible but an indication of the types of costs is as follows:

- Accreditation of security conformity assessment bodies (including testing laboratories) and certification bodies[231]: such bodies - whether existing or created at a future date - will need to be accredited to by a National Accreditation Body[232] and notified to the European Commission[233]. This implies that these conformity assessment bodies may incur costs for the accreditation process (streamlining procedures, audits etc.); normally it is to be expected that such costs will be passed on to their customers in their service price;
- National Accreditation Bodies will incur additional costs for the accreditation of the above conformity assessment bodies[234];
- Additional cost may also be placed on any organisation providing oversight of national level accreditation or, if applicable, oversight of accreditation within sectoral schemes. It is presumed

[231] We make the distinction between certification bodies and conformity assessment bodies, since testing laboratories and other conformity assessment organisations (e.g. inspection bodies) may not be accredited to (directly) provide certification services. See also footnote 224.

[232] Should it be the case that conformity assessment and certification is operated as a sectoral scheme then the process for accreditation should follow the principles set out in Regulation (EC) 765/2008.

[233] This assumes that a future system for accreditation of security conformity assessment and certification bodies will be similar to the procedures under the New Legislative Framework, see Section 7.3.2.

[234] National Accreditation Bodies will themselves be subject to EU-level oversight through the European Cooperation for Accreditation (EA).

that for Type-1 products, such oversight would be provided through the European cooperation for Accreditation (EA) but this does not preclude an alternative arrangement[235].

11.3.4 Impacts for regulators

There are two impacts foreseen for regulators:

- Conformity with EU standards as a basis for national regulations;
- Existence of conformity assessment infrastructure.

Conformity with EU standards as a basis for national regulations {S}

The development and introduction of European Standards and an EU-wide CAC scheme may make it easier for national authorities to introduce national regulations setting product requirements aligned to these standards. On the one hand, regulators will not be required to develop specific requirements/standards but can make reference to European ones. On the other hand, as a conformity assessment and certification will already be in place, regulators will have the assurance that it will be possible to demonstrate conformity with such regulations through the deployment of (EU) certified products.

Facilitation of regulations through existence of conformity assessment infrastructure {E}

For countries that do not possess – or are unable or unwilling to develop - a domestic CAC infrastructure for verifying conformity of security products, the existence of an EU-wide system could remove the need to independently develop such an infrastructure. Instead, with mutual recognition of certification under an EU-wide scheme, they could rely on the CAC infrastructure available in other Member States, thus removing the need to have in place or create their own infrastructure. As such, this may reduce the associated CAC infrastructure costs from introducing regulatory requirements for security products. In turn, this may speed-up the adoption of regulations as there will be lower cost and shorter delay in meeting the corresponding requirements for a CAC infrastructure/scheme to verify compliance with regulations.

11.3.5 Impact for society

It is conceptually difficult to measure the impact that the introduction of an EU-wide conformity assessment and certification scheme would have on society as a whole and on the security of persons, businesses etc. Moreover, it is important to recall that the underlying concerns addressed by Option 1 are primarily related to 'internal market' and 'industrial policy' aspects, rather than (EU) internal security priorities.

As Type-1 products typically address 'continuous' and relatively predictable security threats, it is to expected that increasing the performance of security products should raise overall security levels and, correspondingly, reduce the negative impact of security 'failures' on society. However, in this context the following points may be noted:

- An EU-wide CAC system should raise the average security performance characteristics of deployed products by ensuring that all products meet minimum requirements; i.e. products falling below EU minimum requirements will be removed from the market and already deployed products may be replaced by ones meeting EU minimum requirements. However, there may be risks that a EU-wide CAC system may actually have a negative impact on overall security performance if it reduces incentives for the development of products with performance

[235] Note, Regulation (EC) 765/2008 appears to provide for the possibility of EU financial support for the production and revision of sectoral schemes (Article 32).

characteristics above EU (minimum) requirements (see above 'Minimum standards as *de facto* requirement');

- Notwithstanding the expectation that an EU-wide CAC system would raise the performance characteristics of security products on balance, one should bear in mind that what is important is the overall security system and not just the performance of an individual piece of equipment. The development of an EU-wide CAC system does not remove the fact that security will only be enhanced if the systems (including procedures and processes) are appropriate for the 'subject of protection'. Therefore, CAC for security products does not remove the need to evaluate broader security systems (e.g. *'concepts of operation'*); including whether the products employed within the system are properly integrated and appropriate given the threat/risk assessment.

11.3.6 Technical feasibility

There are currently various national structures for conformity assessment and certification of security products. Option 2.1 would provide for a common (harmonised) EU-wide approach for conformity assessment and certification (hence there will be one umbrella for different security product categories). There are no radical changes to existing structures for CAC foreseen as a consequence. These would rather be brought under a common EU system for approval of conformity assessment bodies. This may result in the exclusion of some of the existing conformity assessment bodies that do not meet the requirements for accreditation under the EU-wide approach. On the other hand, it may be the case that the opportunities offered by the possibility to provide conformity assessment services and EU-wide recognised certification of security products will provide an incentive for new providers to enter the market. With a step-by-step approach it is foreseen that the capacity of the CAC bodies may be able to cope with the additional demand for CAC.

11.3.7 Political feasibility

Option 2.1 may be achieved through a voluntary solution when the market recognises European Standards and duly certified products. In such case no further need for EU intervention would be required other than bringing together the several schemes that exist in Europe. In terms of political feasibility this would be positive.

Manufacturers and suppliers have argued that certification bodies have been slow to embrace EU-wide solutions that would reduce or remove the need for multiple national certifications. Should there be continued consistence on national certification by national certifying bodies or by 'the market', then additional EU intervention may be justified. This could include non-legislative initiatives to promote recognition of European Standards and EU-wide certification, but also a legislative approach might be adopted, in the form of the introduction of specific legislation for security products. A regulatory approach based on the NLF may be problematic if it would relate to the 'security' rather than to the 'safety' aspects of products, which are normally the subject of EU legislation. This was also addressed in Chapter 9.

11.4 Assessment of impacts of Option 2.2 (Step-by-step approach for Type-2 products)

In this section the impacts of Option 2.2 are assessed: a step-by-step approach for introducing EU CAC for 'priority and sensitive' security products (Type-2). These are described for the same five stakeholder types as for Option 2.1:

- Producers;
- Procurers / users;
- Conformity assessment and certification bodies;
- Regulators;
- Society.

Option 2.2 relates to Type-2 products; i.e. products addressing 'priority' threats (e.g. terrorism, organised crime, etc.) often requiring the development or application of new technologies). As many of the impacts from Option 2.2 are similar[236] to those of Option 2.1, it has been chosen not to repeat the analysis of the impact, but to refer to the previous section for a description of that analysis.

Illustration: approval of biometric products

The current situation for security products utilising biometric identification/authentication is illustrative of the type of situation that might be addressed through an EU-wide conformity assessment and certification / approval scheme. This situation may be characterised as follows.

Suppliers of biometric products (e.g. access control devices) are faced by divergent national positions concerning different biometric technologies (e.g. fingerprint, iris, and vein) and also protection of biometric data (e.g. whether a particular technology can be used for authentication and/or identification):

- There is no process in Europe to evaluate the performances, and the robustness to potential fraud, of biometric products. Consequently, potential customers cannot avail themselves of any independent verification of performance and cannot select products based on a solid understanding of the qualities of the products available on the market. This can result in customers purchasing inappropriate or inadequate (low quality) products, with obvious consequences for security performance and also negative effects on customer perception of the technology/industry;
- Authorisation for the use of biometric products is required, however. For example, in France, biometric products are faced with the requirement for a preliminary authorisation by the relevant authority, before products can be used. This can be a long process, characterised by uncertainty as the process is based on general principle which can be interpreted in different ways rather than on clearly defined requirements. This preliminary process is required for each sale of a biometric product;
- Under the French system, the final end-user is responsible for asking for a preliminary authorisation. Inevitably, the end-user turns back to manufacturer for preparing the request for authorisation. At the same time, the complexity of this process, its length and uncertainty drives many potential users to drop the idea of using biometric products, even if they like their potential benefits.

11.4.1 Impacts for producers

Impacts associated with CAC requirements

There are the following impacts identified related to the CAC requirements as a result of option 1:

- Reduction of costs associated to multiple testing to obtain national certification;
- Reduction of the need for client trials;
- Reduction of the 'time to market' of products;
- Reduction of costs associated to adaptation of products to meet different national standards / specifications;
- Enhanced transparency of performance requirements and standards / specifications;
- Acceleration of development process.

[236] Some of the impacts are similar, although these might differ in magnitude; however, it has been proven not possible to assess the magnitudes of the impacts in this study.

Reduction of costs associated to multiple testing to obtain national certification {E}

The impacts are similar to those described for producers of Type 1 products. It can be noted that formal systems for conformity assessment and certification of Type 2 products are relatively poorly developed and cover only a limited number of product categories (e.g. screening equipment for the aviation sector, biometric passports) for which some partial solutions exist for EU-wide conformity assessment (testing) of products. For other product categories for which national authorities require some form of approval, the evaluation of product performance is more often organised on an *ad hoc* basis involving a mixture of testing and operational trials (see below).

Illustration: Conformity assessment and certification of screening equipment

The study has been unable to obtain detailed information on the (direct) costs of testing for Type-2 security products. An industry source has indicated, for example, that the cost of a single test of an Explosive Detection System (EDS) could be in the region of €65 thousand and for a liquid explosive system (LAGS) the figure may vary from €30 to €75 thousand; these figures relate to a single test procedure and do not take into account any repeat testing that may be required. The aforementioned products are relatively small systems and costs associated for larger systems are reputed to be significantly higher and may run into several hundred thousand euros; for example, an amount of €100 thousand has been indicated for an 'imaging test' for a cargo scanner while a figure of €500 thousand has been indicated for the cost of the certification process for a biometric identity card model.

Quantification: The costs of certification and conformity assessment for producers in Europe: the case of airport scanners

In order to quantify the impact of policy option 2.2. regarding the costs of certification and conformity assessment for producers of airport scanners and screening equipment, the first question is how much certification and conformity assessment procedures are currently carried out per year. There is limited information available on that subject. From table 16 above it can be derived that there are at least on average some 20 certifications and approvals of this type of equipment per year. However, this table reflects only the awarded certifications and/ approvals, but does not reflect those products that did not get a certification or approval, and needed multiple re-iterations of the process. Furthermore, it is the certification and approval outcome of only two entities (DGAC and ECAC) in Europe. Therefore, it may be assumed that the annual number of airport scanning and screening products that go into a certification and approval procedure is higher than the 20 mentioned before. A conservative assumption would 30 products, which is used in this study. In reality this could be even higher.

As the market size for airport scanners and screening equipment differs per country, producers will not offer all 30 products for an certification / approval procedure in each of the 27 members states. After all, some small member states with only 1 or 2 airports will not purchase equipment every year, and therefore producers will not or very limitedly enter a certification or approval procedure for new products if they don't expect to sell their products in short term. Apart from that, some countries don't have a formal certification or approval system, but would rely on certification or approval of other member states or ECAC, perhaps with some minor testing of the equipment before implementation. On the other hand there are members states with a large airport scanner and screening equipment market with a more rigorous certification and approval procedure, under which all 30 products may be expected to be offered for certification or approval on average per year. Finally, there is a category of countries in between these two ends of the spectrum sketched above, with a medium sized market for airport scanning and equipment products and a certification and some approval regime that thus does not address all 30 products every year. Based on this the 27 member states have been allocated to three categories, which is presented in the following table.

Category	Airport scanner market size	Member states	Certification and approval regime	Number of countries
1	Large	DE, ES, FR, IT, UK	Full certification and approval of all scanners	5
2	Medium	AT, BG, EL, FI, HU, NL, PL, RO, SE	Some certification and approval half of the scanner	9
3	Small	BE, CY, CZ, DK, EE, IE, LT, LV, LU, MT, PT, SI, SK	Limited certification and approval of few scanners	13
				27

Subsequently, the certification and approval regimes has been further defined. For category 1, full certification and approval of all scanners, it is assumed that thus 100% of the 30 scanners will be certified and approved each year. For category 2, it is assumed that this is 50%, and for category 3 10% is adopted. Furthermore, as outlined above, there may be some variation of the costs of a certification, as this is strongly dependent on the product type. A range from EUR 35 thousand, via EUR 65 thousand, and EUR 100 thousand to even EUR 500 thousand has been mentioned by industry for the certification of a product. The EUR100 thousand relates to a scanner, and this value has therefore been taken in the quantification as a proxy for the costs for a full certification and approval, applying for the five countries in category 1. It has been assumed that the certification and approval process is relatively more light in category 2, and therefore costs have been determined at 50% of the full certification costs, hence at EUR 50 thousand. Finally, costs for certification and approval in category countries have been taken as 10% of the full value, hence EUR 10 thousand. In this latter category it is anticipated that authorities in these countries would heavily rely on the certification and approval of products by large member states, and would require themselves only some limited testing. Based on these assumptions, the baseline annual costs for certification and approval of airport scanner and screening equipment in Europe has been estimated at EUR 22 million, which is further detailed in the table below.

Category	Number of countries	Number of certifications & approvals per year, per country	Number of certifications & approvals per year, in Europe	Costs of certification and approval for producers	Totals costs
Maximum annual number of products for certification and approval		30			
1	5	30	150	EUR 100K	EUR 15 M
2	9	15	145	EUR 50K	EUR 6.75 M
3	13	3	39	EUR 10K	EUR 0.39 M
Total	**27**		**334**		**EUR 22.14 M**

Under policy option 2.2, there is only a single certification and approval process needed for manufacturers for their products. Hence all duplications at national level are prevented, which saves costs. Under the policy option the costs for certification and conformity assessment would thus amount to EUR 3 million (30 products * EUR 100 thousand). **This implies that the impact of the policy option in terms of reduction of costs for certification and conformity assessment amounts to approximately EUR 19 million per year.**

Increase of costs to obtain EU certification {E}

The impacts are similar to those described for producers of Type 1 products. Certification is currently not required for most Type 2 products. Accordingly, the development of an EU framework that sets requirements for such products implies that producers will incur the corresponding costs of conformity assessment and certification of compliance with EU requirements. At the same time, as noted above, currently some form of national approval is often applied to Type 2 products. Accordingly the costs of conformity assessment and certification of compliance with EU requirements should be set against the costs associated to existing *ad hoc* approval mechanisms.

Reduction of the need for product trials {E}

Type 2 products are often characterised by the development and application of new technologies and approaches in reaction to new security threats or aim to enhance security through, for example, automated and integrated systems. Consequently, both public authorities and potential users are particularly concerned to evaluate the performance characteristics of such products (both in terms of 'security' and operational characteristics). Presently, such evaluation is often undertaken through product trials that are typically undertaken *in situ* at the location where the product will eventually be deployed if the trial is successful. These trial periods can last for several months as has been the case, for example, for trial installations of security scanners (a.k.a. body scanners) that are currently being implemented in a number of EU airports.

From a producer perspective, these trials can represent a significant cost burden. The trials imply putting equipment at the disposal of potential clients (and/or authorities) which has not yet been purchased. This implies that producers have incurred the production (and development) costs, which can be substantial, but are able to sell their product only if and when trials are successfully completed. Moreover, in situations in which different clients (or national authorities) require their own product evaluations then this implies that multiple trials may be necessary. More generally, producers are placed in a situation in which public authorities (and/or clients) indicate an interest in having products available to address particular security threats but for which the actual requirements are not clearly specified and the potential market adoption is unclear. This means that there can be a high degree of uncertainty surrounding the potential returns on RTD investments in new security products and technologies.

Under Option 2.2, the definition of common EU requirements and specifications for product performance and an EU-wide scheme for conformity assessment and certification (or approval) should encompass the specification of protocols and procedures for conformity assessment (including product testing and operational trials). Even though such an EU 'package' may still require some form of product trials, the possibility to certify products as being in conformity with EU requirements after an initial trial should reduce the number of trials that products are required to undergo. Specifically, if clients (and/or authorities) have confidence in certification/approval process under and EU-wide scheme then this should remove – or at least reduce – the need for multiple testing/trials. Moreover, an EU 'package' should provide clear indications on the performance criteria to be assessed through testing and product trials and the relevant protocols to be used which, in turn, may reduce the duration of trial periods. Overall, therefore, an EU-wide CAC system with mutual recognition of certificates should result in cost savings for producers.

Reduction of the 'time to market' of products {E}

An EU-wide CAC system with mutual recognition of certification implies that, once a product has been certified as meeting EU requirements, it may be introduced into all EU-markets without the delay caused by the need to obtain national certification/approval. Accordingly, the impacts are similar to those described for producers of Type 1 products.

It should be noted, however, that the conclusion that 'time to market' will be reduced under an EU-wide CAC system with mutual recognition assumes that the time required to define common EU requirements and specifications for product performance and corresponding conformity assessment criteria and protocols does not exceed that required by national authorities/clients. Similarly, it assumes that the time required initiating and implementing product testing and product trials is no more than under exiting *ad hoc* national arrangements. In other words, it presumes that a regulatory process (including definition of product requirements and specification) and operation of an EU-wide CAC system can operate at least as efficiently and rapidly as current approaches.

Reduction of adaptation costs {E}

The impacts are similar to those described for producers of Type 1 products. Essentially, an EU 'package' of legislation and CAC scheme, should provide the basis for more uniform market conditions (i.e. reduced fragmentation), implying less need for producers to adapt products to individual national markets.

Enhanced transparency of performance requirements and standards / specifications {E}

Under Option 2.2, the EU legislative and CAC 'package' should provide clear definition of product requirements and technical standards/specifications. It should set out the performance criteria to be assessed, together with the relevant protocols and criteria to be applied for conformity assessment (and certification). In particular, critical performance and testing parameters should be established and codified. Although access to such information may obviously need to be restricted, it may overcome some of the problems associated to the lack of transparency that producers face in having information on the criteria they are expected to meet in order to obtain approval/certification of their products. Further, it should reduce the potential for performance criteria to be determined during or as part of product testing and trials (see above). Overall, the codification of performance and testing parameters should enable producers to develop their products according to 'predetermined' criteria rather than criteria developed as part of the assessment / evaluation procedure. In turn, this should reduce uncertainty of product assessment / evaluation outcomes.

Acceleration of development process {E}

The introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications should facilitate more rapid product development processes. On the one hand, regulations setting out product requirements and technical specifications should provide producers with a clear indication of the performance characteristics that will be necessary to meet regulatory/market needs. This should make it easier for producers to direct their RTD efforts towards meeting these needs and, also, provide greater clarity/certainty that products meeting EU requirements will be adopted by the market. On the other hand, the existence of a CAC infrastructure may also support the development process. For example, testing laboratories may be involved in an earlier stage of product development (i.e. development testing) where the laboratories themselves will have better information on the criteria and protocols that will eventually be applied to final products. Further, they may be involved in pre-certification testing; i.e. providing partial or preliminary product testing in advance of full testing required for product certification.

Impacts on market conditions

As noted under Option 2.1, the Consultation on an Industrial Policy for the Security Industry carried out by the European Commission indicated that stakeholders observe clear problems in market conditions. The main impacts related to market conditions have been identified and assessed under Option 2.2 are as follows:

- Certification as indicator of product performance;
- Minimum standards as *de facto* requirement;
- Increased competition;

- Increased competitiveness of European manufacturing industry.

These four main impacts have been described for Type 1 products and are valid as well for Type 2 to product. Please refer to section 11.3.1 for a description.

11.4.2 Impacts for procurers / users

There are a number of impacts for procurers and users. As these form the demand side of the market, many of these impacts are related to the impacts as described above under producers. The following impacts have been identified:

- Lower price for security products;
- Increased product choice / availability;
- Enhanced information / transparency on product performance;
- Facilitation of procurement procedures;
- Reduced uncertainty of compliance with (user) security regulations;
- Reduced of need for client trials.

The first five impacts listed above have been described for Type 1 products and are valid as well for Type 2 products. Please refer to section 11.3.2 for a description. Evidently, the magnitude of the impacts may differ between Type 1 and Type 2 products.

Reduced of need for client trials {E}

This impact has been described under the impacts for producers. It is expected that an impact of Option 2.2 will be a reduction in the number of product trials undertaken by clients (and/or public authorities). Apart from a cost reduction for producers, this will also result in a cost reduction for procurers / users as certification will now provide independent verification that products meet EU performance requirements, and hence user's staff will no longer be tied-up in conducting product trials.

11.4.3 Impacts for conformity assessment and certification bodies and system

The following impacts for conformity assessment and certification bodies and the associated infrastructure have been identified:

- Change in the volume of demand for conformity assessment and certification services;
- Increased competition for the provision of conformity assessment and certification services;
- Strengthened EU-wide accreditation;
- Increase of administrative costs related to the CAC system.

Change in the volume of demand for CAC services {E}

Option 2.2 is expected to have two opposite effects on the level of demand for CAC services:

- The introduction of an EU legislative and CAC 'package' that will create a situation in which independent third-party verification of conformity with EU requirements is required for a wider range of product categories than is currently the case. This should increase the volume of demand for conformity assessment and certification services;
- The move towards a system of mutual recognition of certification should reduce the need for multiple conformity assessment (testing etc.) of security products. This should reduce the volume of demand for conformity assessment and certification services.

It is not possible to estimate the net outcome of these two effects.

Competition for the provision of CAC services {E}

In evaluating the possible impact that Option 2.2 may have on competition between providers of CAC services it is important to recognise that the scale of the existing infrastructure for testing of Type-2 products is relatively limited within the EU. For example we can note that only four countries within the EU provide laboratory testing under the ECAC CEP and for testing of biometric passport/identity products/equipment. Similarly, there appears to be limited current capacity for undertaking conformity assessment and certification of other categories of security products/technologies that may be brought under the umbrella of an EU CAC system.

In principle, a 'one stop' EU system for certification should potentially increase competition for the provision of CAC services (as discussed for Option 1 in Section 11.3.3). It is difficult, however, to assess the extent to which this will be realised and how it will impact on the cost and quality of CAC service provision.

Strengthened EU-wide accreditation {E}

As discussed in Section 10.3.3, in order for Member States and other stakeholders to have confidence in an EU CAC system and procedures it will be essential that appropriate checks are made to assure the quality and independence of CAC service providers. This implies a strong emphasis on the accreditation of conformity assessment and certification bodies; this can be expected to be subject to greater critical attention than under Option 2.1. Accordingly, part of the implementation of an EU CAC system for Type-2 products would relate to the development and operation of the infrastructure and procedures for accreditation of conformity assessment (e.g. testing laboratories) and certification bodies.[237] The definition and application of criteria for EU accreditation of CAC service providers should serve to ensure high standards of CAC service provision.

Increase of administrative costs related to the CAC system {E}

The introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications would require the development of a corresponding organisational structure. Section 10.4.2 provides an outline of a possible organisational structure that foresees some additional elements and changes to existing elements of the current CAC actors. This implies some additional administrative costs will be incurred. A detailed costs assessment is not feasible, but some key elements are:

- Security Committee: e.g. staffing and logistic costs;
- EU Body for Security CAC: e.g. staffing, office and logistic costs;
- EU Stakeholder Consultation Group on Security Standards and CAC: e.g. secretariat and logistic costs;
- EU Accreditation of security conformity assessment bodies (e.g. testing laboratories): e.g. costs for the accreditation process (streamlining procedures, audits etc.);
- EU Accreditation of security certification bodies: e.g. costs for the accreditation process (streamlining procedures, audits etc.).

11.4.4 Impacts for regulators

There are two impacts foreseen for regulators:

- Conformity with EU standards as a baseline for national regulations;
- Existence of conformity assessment infrastructure.

[237] See Section 10.4.2 for an outline of a possible organisational structure.

Conformity with EU standards as a baseline for national regulations {S}

The development EU legislation setting product requirements and technical standards / specifications, may provide a framework for national legislation (see corresponding description under Option 1, Section 11.3.4). This may be of particular relevance for Type 2 products (i.e. new and complex technologies) where specific technical knowledge and expertise is required for developing technical standards / specifications.

Existence of conformity assessment infrastructure {E}

The impacts are similar to those described under Option 1 (Section 11.3.4).

11.4.5 Impacts for society

As noted under Option 2.1 it is conceptually difficult to assess the impact of an EU-wide CAC system will have on society and specifically on the security of citizens. This is particularly the case for Type-2 products that address unpredictable security threats. Similar impacts as those described under Option 2.1 (see Section 11.3.5) can be expected in relation to the assurance of minimum standards for security products. Equally the comments regarding the importance of overall security systems and not just the performance of individual products are relevant for Option 2.2. An additional important impact of Option 2 is the possible reduction of 'time to market' for security products (as described in Section 11.4.1). One of the problems identified with existing procedures for defining and implementing standards and conformity assessment procedures for Type-2 products is that they are often too slow to respond to new threats and to technological developments. To the extent that an EU legislative and CAC 'package' can accelerate the deployment of security products to address new threats (or enhance the performance of products to respond to 'existing' threats) it should have a positive impact on security.

11.4.6 Technical feasibility

The technical organisation of the introduction of EU-level structures for type-2 products is discussed in detail in section 9.4.3. This section outlines an organisational structure, taking into account the general absence of existing EU-level structures for defining conformity assessment and certification requirements and procedures for type-2 products. This structure would include:

- Security Committee;
- EU Body for Security CAC;
- EU Stakeholder Consultation Group on Security Standards and CAC;
- EU Accredited Security Testing Laboratories;
- EU Accredited Security Certification Bodies.

It is considered that if this proposed structure is applied, the implementation of policy option 2.2 could be technically feasible. It has already been described above that there are costs associated with implementing the organisational structure.

11.4.7 Political feasibility

Type 2 products are characterised by their link to new threats, application to important and dynamic security functions such as border control, advanced and innovative designs and their link to issues of national concern. As a result, national governments are likely to want to maintain a certain level of influence in the development and use of such products within their borders. The introduction of an EU-wide scheme for a number of these products may therefore be politically sensitive. It would require mutual agreement between the EU and the individual Member States to decide which products would be included in an EU-wide conformity assessment and certification scheme.

11.5 Assessment of impacts of Option 3 (all-encompassing approach)

In this section the impacts of an all-encompassing approach of an EU-wide CAC system for all security products (hence type 1 and type 2) are assessed.

11.5.1 Impacts

This is the most far-stretching option, where an EU-wide CEC system is in place for all security products. In sections 11.3 and 11.4 the impacts are described for products of type 1 and type 2, in a step by step approach where some products are subject to conformity assessment and certification procedures, and others are not. It is considered that the impacts for this third policy option with an all-encompassing approach would be *the same*, but the *magnitude* of the impacts would be much larger due to the fact that here all security products are included.

Obviously, the extent to which this magnitude would be larger is very difficult to assess. For that, it would be required to know exactly how many security products there are in all EU Member States, but also those products from e.g. China, USA and Japan that are purchased by users from the EU and all the costs involved in the conformity assessment and certification procedures, as well as any other costs and benefits related to this. This information is not available.

In general, it is foreseen that the most important additional impact of this option compared to the second option will be in the impacts associated with CAC requirement and market conditions for producers, the impacts for user/ procurers, and the impacts for conformity assessment and certification bodies. Here, one could claim that the increase in number of products that are covered by the all-encompassing EU-wide conformity assessment and certification system will almost directly be the increased magnitude of the impacts compared to the impacts of option 2.1 and 2.2. It is more difficult to indicate this for the impact for regulators, as national regulations on conformity procedures are more interwoven in other policies and regulations and it is difficult to single out the exact impact of additional products falling under the EU-wide scheme.

11.5.2 Technical feasibility

Technically it will be very difficult to introduce an EU-wide scheme for all security products. A first issue is to determine which products fall within the ‘security’ sector, and for instance not under ‘safety’. Subsequently, there may be implementation difficulties with the all-encompassing policy option. A clear barrier is that it will address a large number of products that will need to be certified. It is questionable whether the existing CAC infrastructure would be able to cope with the additional volume, even if it is unclear now what the exact volume is of current CAC procedures in Europe.

11.5.3 Political feasibility

In terms of political feasibility, a combination of what is discussed under options 2.1 and 2.2 applies. For products of Type 1, political feasibility is considered to be relatively high, as there are no clear political barriers identified. Obviously, Member States would need to address the above described issue of the technical feasibility though and the associated question on the funding for scoping the CAC infrastructure to the required level. The political feasibility of applying the option for all products of Type 2 seems to be relatively lower. The foreseen organisation structure implies a significant change compared to the current situation, and the character and nature of the type-2 products will make this option very sensitive. It is foreseen to lead to reluctance of Member States to adopt the option.

11.6 Summary

The following table provides a summary of the impacts as described in the previous sections. The table is structured according to the five stakeholder groups. As option 1 is the baseline (do-nothing) against which options 2.1, 2.2 and 3 are evaluated, the impacts have been put to '0', to express the change if one of the options would be implemented.

	Impact	Option 1 Base line	Option 2.1	Option 2.1	Option 3
	PRODUCERS				
	Reduction of cost associated to multiple testing to obtain national approval/certification: • Single certification of compliance to EU requirements recognised across Member States.	0	+	+	++
	Increase of costs to obtain EU certification: • Single certification of compliance with EU requirements needed for products.	0	-	-	--
	Reduction of 'time to market': • Certified products can be supplied to all markets without delay caused by additional national approval/certification.	0	+	+	++
	Reduction of costs associated to adaptation of products to meet different national standards/specifications: • Products certified to common agreed EU standards/specifications; • Single 'product model' accepted throughout EU market; reduced production efficiency/costs from removal of need to supply national variants.	0	+	+	++
	Enhanced transparency of performance requirements and standards/specifications: • Performance requirements, and corresponding standards/ specifications and testing protocols are codified; • Producers/suppliers able to develop products according to 'pre-determined' criteria rather than criteria developed as part of the assessment/evaluation procedure; • Reduced uncertainty of product assessment/evaluation outcomes.	0		+	++
	Certification as an indicator of product performance: • Certification provides independent verification that product meets EU performance requirements; • Facilitates market acceptance (especially SMEs, new-entrants etc.), reduced 'reputation' effect.	0	+	+	++
	Reduction of need for client trials: • Certification provides independent verification that product meets EU performance requirements; • Equipment and staff not tied-up by client trials.	0		+	++
	Acceleration of development processes: • Products can be tested according to agreed test protocols and against EU performance requirements during the	0		+	++

	Impact	Option 1 Base line	Option 2.1	Option 2.1	Option 3
	development phase.				
	Market adopts minimum standards as *de facto* requirement: • Market (users) procurement based on minimum performance requirements (i.e. products certified in compliance to EU minimum specifications); • Reduced attractiveness of developing products with performance above EU minimum specifications.	0	-	-	--
	Competition: • Increased market transparency (products conform to common EU standards); • Increased market openness (lower barriers to market entry): - EU and non-EU suppliers ; - SMEs / New business start-ups.	0	+	+	++
	Competitiveness of EU suppliers: • Reduced 'protection' of national markets (productivity improvement from increased competition); • Increased innovation (return from innovation increased through wider EU market access); • European certification as a recognised international 'quality' label.	0	+	+	++
	PROCURERS / USERS				
	Lower price for security products (pass-on from producers): • Lower conformity assessment / certification costs; • Lower cost through production efficiency and scale economies; • Lower cost from increased market competition.	0	+	+	++
	Increased product choice / availability: • Increased market openness (more suppliers / products on national markets); • Increased availability of new technologies / innovative solutions.	0	+	+	++
	Enhanced information / transparency on product performance: • Product certification as indicator of product performance.	0	+	+	++
	Facilitation of procurement procedures: • EU standards/specification and certification as a requirement in procurement contracts; • EU wide procurement possibilities (e.g. same products/systems compliant in different national markets, economies of scale in procurement, single suppliers, etc.).	0	+	+	++
	Reduced uncertainty of compliance with (user) security regulations: • Product certification as indicator that security equipment/systems meet regulatory (or other) performance requirements.	0	+	+	++

	Impact	Option 1 Base line	Option 2.1	Option 2.1	Option 3
	Reduction of need for client trials: • Certification provides independent verification that product meets EU performance requirements; • Staff not tied-up conducting product trials.	0		+	++
	CONFORMITY ASSESSMENT & CERTIFICATION BODIES & SYSTEM				
	Reduced volume of demand for CAC: • Products certified in compliance to EU requirements do not need further national certification.	0	-		--
	Increased volume of demand for CAC: • New products (or products previously not covered by CAC requirements) brought within EU scheme.	0	-	-	--
	Increased competition for the provision of CAC services: • National (closed) markets for CAC opened up to international competition; • Price competition (lower price for CAC services); • Quality/service competition (time, information supply,).	0	-/+	-/+	--/++
	Increase of administrative costs: • Costs incurred by different stakeholders in the CAC system as a result of implementing the policy option.	0	-	-	--
	REGULATORS				
	Conformity with EU standards as a baseline for national regulations: • Regulators enabled to tune their national regulations to the EU standards / performance requirements.	0	+-	+/-	++/--
	Existence of conformity assessment infrastructure: • Reduced need to set-up CAC infrastructure.	0	+	+	++
	SOCIETY				
	Security positively affected: • Decrease of products with performance below EU minimum performance requirements; • Market adopts minimum standards as de facto requirement; • Overall security level increase through accelerated introduction of security products answering new threats.	0	+	+	++

References and literature

Articles, studies and reports:

- Alderman, D.F., 'The US Government's role in standards and conformity assessment', presentation June 2, 2008;
- ANSI, 'The United States Standards Strategy (USSS)', 2005;
- ASD and EOS, Joint ASD/EOS proposal on EU Third Party Liability Limitation;
- Common Criteria, 'Common Criteria for Information Technology Security Evaluation', Version 3.1, July 2009;
- Benda, P., "Unlocking the SAFTEY Act's potential to promote technology and combat terrorism', Testimony of Acting Deputy Under Secretary of the DHS, May 2011. See: http://www.dhs.gov/ynews/testimony/testimony_1306419295690.shtm;
- Biagin, R.B., ' Involving the SAFETY act: a matter of corporate responsibility and competitive edge', The Procurement Lawyer, volume 39 (3), p. 23-26, spring 2004;
- Carafano, J.J., ' Fighting terrorism, addressing liability: a global proposal', Backgrounder, published by the Heritage Foundation, May 21, 2008;
- DHS, 'DHS's role in state and local fusion centres is evolving', December 2008;
- DHS, 'Fiscal Year 2011 – Budget in Brief', 2010 (undated);
- DHS, 'Quadrennial Homeland Security Review', February 2010;
- DHS, 'Department of Homeland Security 2010 Accomplishments & Reforms', December 2010;
- Ecorys, 'Study on the competitiveness of the EU security industry', November 2009;
- Ernst D. and S. Martin (2010), 'The Common criteria Information Technology Security Evaluation – Implications for China's Policy on Information Security Standards', East-West Centre Working Paper, No 108, January 2010;
- European Court of Human Rights, Factsheet 'Protection of Personal Data', June 2011;
- European Forum for Urban Security, 'Charter for a democratic use of video-surveillance', 2010;
- European Union Institute for Security Studies, 'Towards a European Defence Market', Chaillot Paper No. 113, November 2008;
- Gordon Gillerrman, 'Making the Confidence Connection: Conformity Assessment System Design', 2005;
- Gordon Gillerman, 'Conformity assessment practical implications', (InterAgency Committee on Standards Policy), June 2007;
- Gordon Gillerman, 'Conformity assessment, regulation and standards and trade' presentation July 2008;
- Greenberger, M., ' Teaching new dogs old tricks: reshaping the department of homeland security's technology development infrastructure', Jurimetrics, volume 47, p. 281-296, spring 2007;
- Kushnier G.W. (ANSI), 'Overiew of the US Standards and conformance systems', presentation, 2007;
- Levin, A.M., 'The SAFETY Act of 2003: implications for the government contractor defence', Public Contract Law Journal, Volume 34 (1), p. 175-205, Fall 2004;
- Lim, Laurent, 'The legislative framework of video surveillance in Europe' in European Forum for Urban Security, "*Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV",* 2010;
- Lowell, S., 'Defence Standardisation Program', presentation June 2008;
- NCSA, 'Common Criteria Reforms: Better Security Products through Increased Cooperation with Industry', 2011;
- NIST, 'The ABC's of the US conformity assessment system', April 1997;

- NIST, 'Summary of the Responses to the National Science and Technology Council's Sub-Committee on Standards Request-for-Information, "Effectiveness of Federal Agency Participation in Standardization in Select Technology Sectors"', December 8, 2010;
- Oliver, W.M., 'Policing for Homeland Security: Policy & Research', in: Criminal Justice Policy Review, 2009 (20);
- Pavlick, J.J., Locaria, D.N., 'Final SAFETY Act rule resolve some questions, generates others, and creates important procurement linkage to the SAFETY Act', the Procurement Lawyer, Volume 42 (1), fall 2006;
- President of the United States, 'National Strategy for Homeland Security', May 2010;
- Purcell, D.E. 'Strategic Standardisation' 2008, http://www.strategicstandards.com/Perspectives.html;
- Tanenbaum, W.A., ' Updating key contract terms in business process, IT and offshore outsourcing, in: The outsourcing revolution, 2003;
- Taylor, A.C., 'Government contractors: above the laws of war?', Public Contract Law Journal, Volume 35 (2), p. 281-295, Winter 2006;
- Thomas, J., 'International Standards and Trade', presentation July 9 2009;
- UK Department for Business, Innovation and Skills (BIS) 'Guidance for officials: avoiding new barriers to trade, Directive (as amended by Directive 98/48/EC)', September 2009;
- U.S. Congress, Office of Technology Assessment, Global Standards: 'Building Blocks for the Future', TCT-512, Washington, DC: U.S. Government Printing Office, March 1992;
- US Department of Transportation, 'Voluntary industry standards and their relationship to government programs', 1993;
- Zhou C. and S. Ramacciotti, 'Common Criteria: Its limitations and advice on improvement', ISSA Journal, April 2011.

EU Institutions' documents:

- European Commission, OLAF, 'ECJ Decisions relating to data protection', June 2010;
- Council of the European Union, 'Internal Security Strategy, Towards a European Security model', 23 Feb 2010;
- Council of the European Union, 'A Secure Europe in a Better World. European Security Strategy', 2003;
- Council of the European Union, 'The European Union Counter-Terrorism Strategy', 2005;
- Council of the European Union, 'The Stockholm Programme', 2009;
- Council of the European Union, 'EU Plan of Action on Combating Terrorism', 2001;
- European Commission, Communication 'A comprehensive approach on personal data protection in the European Union', COM(2010) 609 final, 4 November 2010;
- European Commission, Communication 'The EU Counter-Terrorism Policy: main achievements and future challenges', COM (2010) 386 final, 20 July 2010;
- European Commission, Communication 'on the Use of Security Scanners at EU airports, COM(2010) 311 final, 15 June 2010;
- European Commission, Communication 'Action Plan of the Stockholm Programme', COM(171) 210 final, 20 April 2010;
- European Commission, Communication 'Protecting Europe from large scale cyber-attacks and disruption: enhancing preparedness, security and resilience', COM(2009)149, 30 March 2009;
- European Commission, Communication 'Follow-up of the Work Programme for better implementation of the Data Protection Directive', COM(2007) 87 final, 7 March 2007;
- European Commission, Communication 'Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement' COM (2006) 779, 7 December 2006;
- European Commission, 'A guide to the procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services', 2005;

- European Commission, Communication ‘Critical infrastructure protection in the fight against terrorism’, COM(2004)702 final, 20 October 2004;
- European Commission, Communication on the role of customs in the integrated management of external borders, COM(2003) 452 final, 21 April 2004;
- European Commission, ‘Guide to the implementation of directives based on the New Approach and the Global Approach’, 2000.

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

Watermanweg 44
3067 GG Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com

W www.ecorys.nl

Sound analysis, inspiring ideas