Transilvania University of Brasov,
Romania

13th INTERNATIONAL CONFERENCE
"STANDARDIZATION, PROTYPES AND QUALITY:
A MEANS OF BALKAN COUNTRIES' COLLABORATION"

Brasov, Romania, November 3 - 4, 2016

A Concise Survey of Security Standards and Certification Services

Dr. POUSTOURLI Aikaterini
Technological Educational Institute of Central Macedonia, Serres – Greece, pkate@teiser.gr

Abstract

After the terrorist events in Paris and Brussels, it is considered more than ever crucial and essential for the European Union to proceed in a cohesion, close cooperation and establishment of a common language on security topics. A number of international standards to achieving the goals of the Europe 2020 strategy in terms of smart, sustainable and inclusive growth. Taking into account that Standards facilitate innovation by providing a balance between collaboration and competition, the existent and the ongoing security standards and certification schemes are oriented and focused to deal with the demands and the trends of the new era regarding the technological evolutions, threats, risks. This work is a literature review, a concise survey on the main European and United States certification services, organisations and standards. The challenge of robust and mutual beneficial collaborations internationally in transatlantic level is considering fundamental for many policy makers and security stakeholders. Scientist share their agony for joining contributions and efforts in order to achieve robustness and resilience in European and global environment that will lead in smart and resilient societies in a better world for the future generations.

Keywords

standardisation, security, critical infrastructures protection, research, certification, accreditation, quality schemes, conformity assessment, harmonisation, standards, normative documents

1. Introduction

The paper identifies the main organisations for security certification schemes and standards in USA and in the EU. The lack of EU legislation for certification schemes is to a certain extent covered by the international and European standards and the guidance from standardisation bodies. With regard to the security legislation framework, the EU and the Member States share competence in the area of security. The security legislation in the EU is sector-specific and provides useful insight as to requirements for security products and services. Demands relate to physical controls and training of personnel, as well as the performance and the functioning of the security equipment. The multi-layered risks of physical and digital nature urge for accountability, security and risk assessments. Access to information systems and prevention from illegal interception and interference to the data and systems are also significant requirements incorporated to the EU legislation.

Certification means guarantee of quality and evidence for conformity to a third independent party regarding products, systems, services and people. In general, the supplier can assess and declare the conformity of its product to requirements of a normative document, such as a standard, by herself. Certification however is performed by third parties, independent certification bodies which after performing an audit, they issue a certification for compliance of a product, service or person with specific requirements. In that case, the impartiality and independence of the third party are crucial for the credibility of the certificate, which will be issued. It is the certification scheme, which sets the rules, requirements and methodology on how the process will take place and what the end result will be. The certification scheme may seek to provide the product with a certificate of compliance with a standard. It might be the case instead, that a scheme is based on other normative documents or legal provisions, or both. **Conformity assessment** refers to the acknowledgement that a product, a system, a person or a board fulfils a set of fixed requirements (EN ISO/IEC 17000:2005). There are various conformity assessment bodies, such as test laboratories, calibration units, and inspection units in addition to certification and verification bodies. All confirm that the needed requirements are achieved. Those requirements are usually set through standards, laws, specifications and voluntary agreements among parties. On this basis, obtaining a certificate is proof that a product complies to (or "conforms with") specific legislation or other technical specifications or criteria.

Standardisation takes place on three different levels. **Worldwide** standards are developed by ISO (International Organization for Standardisation), IEC (International Electrotechnical Committee) and ITU (International Telecommunication Union). **European** standards are developed by CEN (European Committee for Standardisation), CENELEC (European Committee for Electrotechnical Standardisation) and ETSI (European Telecommunications Standards Institute), also called the three "European Standardisation Organisations" (ESOs). Throughout this document, whenever ISO is mentioned, this also included IEC and whenever CEN is mentioned, this also included CENELEC. The third level of standardisation is the **national** level. Most countries in the world and all European countries have one National Standardisation Body (NSB). Differences in standards and technical regulations between countries, "even when justified, may sometimes create technical barriers to trade".8 On the other hand, a number of empirical studies highlight the positive effect of harmonized national standards on trade.
Members of CEN and CENELEC are the NSBs from every EU Member State, the Former Yugoslav FYROM, Turkey and the three countries of the European Free Trade Association (EFTA) – Iceland, Norway and Switzerland. The case of ETSI is different however. In ETSI Committees individuals, user groups and especially corporate organizations are members and not national representatives. All ISO standards are voluntary in use and in adoption.

The rules for adopting European standards on a national level differ from the rules for ISO standards. The European standardisation system is unique in the world. After the publication of a European Standard, each national standards body or committee is obliged to withdraw any national standard that conflicts with the new European Standard. Hence, one European Standard becomes the national standard in all the 33 member countries of CEN and/or CENELEC. As soon as CEN decides to adopt an ISO standard as an EN, this document automatically has to be adopted by the member countries as well and becomes, for example, DIN-EN-ISO. A majority of European Standards are initiated by business and developed in partnership with other stakeholders. Around 30% are mandated by the European Commission in the framework of EU legislation. Following the plurality of notions of security, the EU legislation uses the term in several contexts. Not every legal text relating to security however is of use for this analysis. The analysis below will present the main legal texts at EU level that are related to security. The presentation will follow the areas of security as in CRISP glossary, which are:

- Security of Citizens
- Security of Infrastructures
- Border Security
- Crisis Management.

For the above four security domains there are respectively eleven different relative functions, which are the Detect, Locate, Track, Assess, Identify, Verify, Authorise, Control, Create Situational Awareness, Detain and Prevent/Protect.

2. Existing Inventories for Security Standards and Certification Schemes

2.1. Security standards from International Organisation for Standardisation (ISO)

The ISO inventory for security related standards was prepared by ISO Strategic Advisory Group on Security (SAG-S). The SAG-S issued a call to ISO members, the International Electrotechnical Commission (IEC) and the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) asking that they provide standards in the field of security. This inventory of standards has been divided into three broad areas of security dealing with targets, threats and timelines.

2.1.1. Targets

This inventory is limited to those standards associated with *targets* – people, infrastructure and other assets – that may be vulnerable to security threats. This inventory of security targets standards and specifications identifies a collection of documents (which it refers to as standards even though they encompass more than traditional ISO, IEC and ITU standards) that provide guidance on meeting the needs posed by organizations concerned about security threats from man-made or natural disasters. While its primary audience is standards developers, it can also be helpful for developers of products and services and policy makers in the security field. The main taxonomy of standards in the category of Targets ISO Inventory are as bellow:

Food and Agriculture

Food and agriculture as a target includes agricultural production services, animal producers, plant producers, food processors and manufacturers, restaurant and food service companies, and warehouse and logistics facilities. Standards entries here are subdivided into

- Food and
- Agricultures

Water

The water target includes public drinking water and water supply pipelines, wastewater systems (treatment plants and management), irrigation (dams, channels, canals) and storm water drainage systems. Standards entries here are subdivided into

- Water Supplies,
- Drinking Water and
- Wastewater.

Energy

The energy target consists of thousands of geographically dispersed electricity, oil and natural gas assets that are connected by systems and networks. The energy target includes specific assets such as SmartGrid and nuclear power plants. The entries here are subdivided into three major categories:

- Electric Utilities,
- Nuclear Energy and
- Oil, Gas and Pipelines.

Information and Communications Technology (ICT)

The ICT target includes voice, video, internet as well as data services and systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on one another to carry and terminate their traffic, and companies routinely share facilities and technology with one another to ensure interoperability. This target also includes the reliable operation of networks and systems and the movement and storage of critical data. Other aspects of this target sector include incident-management communications; domain-name resolution services; Internet-based content and information; Internet routing, access and connection services. Subcategories in this broad target area are likely to expand, but the initial set is

- Identification Cards,
- Information Security and Healthcare Informatics,
- Biometrics and
- Communications.

Industrial Base

The industrial base is composed of several broad manufacturing industries. These industries include, but are not limited to chemical and petrochemical facilities; primary metal manufacturing; machinery manufacturing; electrical equipment and IT component manufacturing; and transportation equipment manufacturing. This target also includes the thousands of worldwide industrial facilities with varying capabilities to perform, research and development, design, produce, deliver and maintain military weapons systems, subsystems, components, or parts for the military infrastructure. The industrial base target is subdivided into

- Modeling, Simulation and Analysis,
- Intrusion Prevention, Sensors and Detectors,
- Fire Prevention and
- Heating, Ventilation and Air Conditioning.

Public Safety, Emergency Services and Healthcare

This target includes first responder and emergency medical services provided to the public in the face of manmade and natural disasters. It also includes hospitals, clinics and ambulatory care, blood banks, population-based care provided by health agencies, and pharmaceutical research and manufacturing companies. Standards entries here are subdivided into

- Public Safety,
- Emergency Services and
- Healthcare

(Security standards for Healthcare Informatics are covered in an IT section).

Transportation

The transportation and logistics target includes all the modes of transportation that move tens of millions of passengers and trillions of US$ in goods in a vast interdependent network. This target includes roads and highways, railroads, bridges, tunnels, seaports, airports, waterways, train stations, mass transit venues. This target sector is subdivided into

- Infrastructure,
- Intermodal and Rail,
- Maritime (3.7.3) and
- Air Cargo.

Two additional subcategories are devoted to standards for tools used to inspect and track assets in transportation and logistics networks: Radiofrequency Identification Devices (RFID) and X-ray Inspection Systems.

Mass Gatherings

The mass gathering target includes facilities that operate on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers. The sector comprises subsectors including lodgings, resorts, government buildings, commercial office buildings, convention centers, stadiums/arenas, theme parks, schools, and church/religious centers. This target is subdivided into

- Public Places and
- Special Events and Sports Venues.

2.1.2. Threats

This inventory is limited to those standards associated with security threats. This inventory of security threat standards and specifications identifies a collection of documents (which it refers to as standards even though they encompass more than traditional ISO, IEC and ITU standards) that provide guidance on meeting the needs posed by organizations concerned about security threats from man-made or natural disasters. While its primary audience is standards developers, it can also be helpful for developers of products and services and policy makers in the security field. There are many possible means of organizing the set of standards identified in this document. The approach taken here is to categorize security standards in terms of threats, in terms of chronology of an event (timelines) and in terms of targets of a terrorist attack or infrastructure that must be protected from natural disasters. This organization does not provide mutually exclusive categories, but rather categories that can be added together to provide increasingly detailed guidance to users. Standards will be listed in all areas that apply, and standards concerned with risk management may well appear in two or three of the categories.

Chemical, Biological, Radiological/Nuclear and Explosives (CBRNE) threats

Chemical, Biological, Radiological/Nuclear and Explosives (often abbreviated to CBRNE) is protective measures taken in situations in which any of these four hazards are present. CBRNE standards address products and services that relate to detection, personnel protection, decontamination, and mitigation.

- **Chemical threats:** Includes warfare agents, toxic industrial chemicals, toxic industrial materials, aerosol dispersion, water contamination, tank cars (Cl2), chemical plants, release of chemicals, and hazardous materials.
- **Biological threats:** Includes agent itself, viruses (ex. H1N1), proteins/toxins (ex. Ricin) and bacteria (ex. *Bacillus anthracis*) and outcomes such as pandemics or infestations.
- **Radiological/Nuclear threats:** Includes fission products (spent fuel), medical isotopes and industrial isotopes, and special nuclear material.

- **Explosives threats:** Includes conventional military and industrial explosives, ANFO (ammonium nitrate/fuel oil), and homemade (TATP) and precursors to homemade explosives.

Cybersecurity threats

Cybersecurity includes disruptive activities, or the threat thereof, against computers and/or networks, with the result of harm.

Criminal threats

Standards which relate to criminal threats, excluding cyber threats which are in their own separate category, are those intended to aid in identifying criminals such as biometrics standards and those that categorize criminal activities such as fraud and counterfeiting.

Natural Disasters

Natural disasters present a wide range of threats to the populace. Standards for the natural disaster threats are subdivided here into categories of Geological Hazards and Meteorological Hazards. Many of these recurring disasters can be anticipated based on historical records and increasingly accurate forecasting methodologies. Target communities may identify more specific guidance on standards in the Targets and Timelines Collections.

- Geological Hazard threats (they include: Earthquakes, tsunamis, volcanoes, landslides, mudslides, subsidence, glaciers and icebergs).
- Meteorological Hazard threats.

2.1.3. Timelines

This inventory is limited to those standards associated with *timelines* – that is, standards associated with the temporal dimension of a large scale natural disaster or terrorist attack. This inventory of security timelines standards and specifications identifies a collection of documents (which it refers to as standards even though they encompass more than traditional ISO, IEC and ITU standards) that provide guidance on meeting the needs posed by organizations concerned about security threats from man-made or natural disasters. While its primary audience is standards developers, it can also be helpful for developers of products and services and policy makers in the security field. There are many possible means of organizing the set of standards identified in this document. The approach taken here is to categorize security standards in terms of the temporal *timeline* of a terrorist attack or natural disaster, in terms of targets, and in terms of security threats. This organization does not provide mutually exclusive categories, but rather categories that can be added together to provide increasingly detailed guidance to users. Standards will be listed in all areas that apply, and standards concerned with risk management may well appear in two or three of the categories.

Preparedness

Preparedness is the first overlapping phase that covers analysing, planning, resources, training, exercising, impact reduction, validation and organization of organizational capabilities. In this Timelines Collection, *Preparedness* has subcategories for

- Training and
- Equipment.

Response

Response is the second overlapping phase that covers the immediate actions to save human life, protect property and the environment, and meet basic human needs. This also includes the execution of emergency plans and actions by incident managers. In this Timelines Collection, *Response* has several subcategories:

- Communications
- Incident Management
- Personal Protective Equipment
- Equipment

Recovery

Recovery is the third overlapping phase that generally covers the actions of trained technical personnel to triage the incident scene. These will include law enforcement officers to collect evidence, public utility technical staff to restore power, communications, water and transportation, and hazardous materials specialists to decontaminate personnel as well as critical facilities.

Remediation

Remediation is the last overlapping phase that returns the organisation or 'environment' back to normality or a new normality, and attempts to enhance the capability of the organization or 'environment' to withstand future comparable incidents.

2.2. Security standards from National Institute for Standards and Technology for Standardisation (NIST, USA)

NIST has brought together major stakeholders from the retail and security industries, computer vision technologists/developers, the research community, law enforcement, and government agencies in a common mission to advance the state-of-the-art in predictive video analytics. The focus of the VISITORS project is to advance technologies and methodologies used to detect persons engaged in suspicious activities as applied in the retail domain. The initial "meeting of the minds" was held via a technical symposium in June 2010 to identify interest and key issues among the stakeholders. The resulting roadmap indicating the pathway ahead is now available. From helping to develop technologies that detect explosives and locate survivors in a collapsed building to video software that identifies criminals and high endurance building materials, the National Institute of Standards and Technology (NIST) is working to keep people safe. The main four subject areas are included in the Public Safety/Security Portal:

- Consumer Safety
- First Responder
- Homeland Security
- Law Enforcement

2.2.1. Consumer safety

Support of Industry Compliance with the EU Directive on Restriction of Certain Hazardous Substances (RoHS)

The Chemical Sciences Division is involved in development of standards and reference materials for restricted hazardous substances through participation in international test method development programs, by providing existing Standard Reference Materials (SRMs) for test method validation, and by investing in development of new SRMs. Chemical Sciences Division involvement with RoHS is based in large measure on feedback obtained during a NIST workshop in October 2005, which resulted in a prioritized list of materials for new SRMs. Current projects include production of SRMs for lead-free solder and free-cutting brass containing high levels of restricted substances. Collaborations are underway with the National Institute of Metrology of China (NIM-C) and the Institute for Reference Materials and Measurements (IRMM) of the European Union (EU).

Support of the Consumer Products Safety Improvement Act (CPSIA) of 2008 – Lead in Paint on Toys: After enactment of the CPSIA, a collaboration was established between the Consumer Product Safety Commission (CPSC) and NIST.

Video Surveillance Technologies for Retail Security (VISITORS)

NIST has brought together major stakeholders from the retail and security industries, computer vision technologists/developers, the research community, law enforcement, and government agencies in a common mission to advance the state-of-the-art in predictive video analytics. The focus of the VISITORS project is to advance technologies and methodologies used to detect persons engaged in suspicious activities as applied in the retail domain. The initial "meeting of the minds" was held via a technical symposium in June 2010 to identify interest and key issues among the stakeholders. The resulting roadmap indicating the pathway ahead is now available.

2.2.2. First responder portal

Calibration of Beta-Particle Sources and Instruments for Radiation Protection

A calibration service for protection-level beta-particle sources and instrumentation has been in place at NIST for several years.

Metrology and Standards for Canine Olfactory Detection of Explosives

As part of a multi-year interagency agreement between the Office of Standards of the Department of Homeland Security and NIST.

700 MHz Band Channel Propagation Model

To provide telecommunications designers working in public safety communications with channel propagation models to use in simulation and testing.

NIST Test Bed for Explosives Trace Detection

The NIST Entry Point Screening Test Bed conducts fundamental research to generate measurements and standards that address critical challenges.

Polymer Microspheres by Annular Co-Flow Extrusion

Well characterized test materials are essential for validating the performance of trace explosive detection systems.

2.2.3. Homeland security portal

Main Subject Areas are:

- Chemical/Biological/Radiological/Nuclear/Explosives (CBRNE)
- Critical Infrastructure Protection (CIP)
- Cybersecurity
- National Construction Safety Team Investigations

The relative Programs and Projects include:

Development of NIST Standard Reference Materials for Trace Explosives Detection

As part of a multiyear interagency agreement between NIST and the Office of Standards of the Department of Homeland Security, NIST is developing a

Cyber-Physical Systems for Global Cities Project

Cyber-Physical Systems (CPS) provide cities with a pathway to enhance and integrate key infrastructures and systems to dramatically improve.

Cyber-Physical Systems Testbed Design Concepts Project

A key challenge to progress in cyber-physical systems (CPS) is the lack of robust platforms for experiment and testing, which NIST is addressing.

Reference Architecture for Cyber-Physical Systems Project

Cyber-Physical Systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. CPS

Cybersecurity for Smart Manufacturing Systems

The Cybersecurity for Smart Manufacturing Systems project will deliver a cybersecurity risk management framework with supporting guidelines.

Standard Test Methods for Response Robots

The U.S. National Institute of Standards and Technology (NIST) is developing a comprehensive set of standard test methods.

2.2.4. Law enforcement portal

Subject Areas

- Ballistics
- Biometrics
- Communications
- Forensics
- Weapons & Protective Systems

The main relative Programs and Projects are:

Development of NIST Standard Reference Materials for Trace Explosives Detection

As part of a multiyear interagency agreement between NIST and the Office of Standards of the Department of Homeland Security.

Metrology and Standards for Canine Olfactory Detection of Explosives

As part of a multi-year interagency agreement between the Office of Standards of the Department of Homeland Security and NIST.

Personal Body Armor

Our goal is to prevent the catastrophic failure of ballistic body armor by developing measurements and predictive models to test.

NIST Test Bed for Explosives Trace Detection

The NIST Entry Point Screening Test Bed conducts fundamental research to generate measurements and standards that address critical challenges.

Public Safety Communication Systems

The primary objective of the Public Safety Communications Research program is to lead the development of wireless telecommunications.

Video Surveillance Technologies for Retail Security

NIST has brought together major stakeholders from the retail and security industries, computer vision technologists/developers, the research etc.

2.3. Organization of Scientific Area Committees (OSAC) Catalog of External Standards and Guidelines

OSAC is part of an initiative by NIST and the Department of Justice to strengthen forensic science in the United States. The organization is a collaborative body of more than 500 forensic science practitioners and other experts who represent local, state, and federal agencies; academia, and industry. NIST has established OSAC to support the development and promulgation of forensic science consensus documentary standards and guidelines, and to ensure that a sufficient scientific basis exists for each discipline. The OSAC Catalog of External Standards and Guidelines is a collection of standards, guidelines and other documents applicable to forensic science. None of the documents in the catalog have been developed or approved by OSAC (the Organization of Scientific Area Committees). NIST staff compiled the catalog in early 2015 for OSAC members to assess existing standards, guidelines and best practices that are already publicly available. OSAC committees may propose standards and guidelines from the catalog to submit for inclusion in the OSAC Registry of Approved Standards or OSAC Registry of Approved Guidelines, only after following a rigorous OSAC approval process. They may also develop new standards and guidelines for the OSAC registries to replace current documents in the catalog. They may also develop entirely new and original standards and guidelines. OSAC subcommittees met in early 2015 to review the Catalog of External Standards and Guidelines and to begin determining priority needs. It contains the titles and source information for more than 700 standards, guidelines and related documents. The catalog also lists web addresses for documents that are available online.

2.4. Telecommunications Security Group (TSG) standards, USA

The Telecommunications Security Group (TSG) is a Joint Working Group of the Committee on US National Security Systems (CNSS) that was established under the EO 13231 committee to protect the US National Security Systems. Main series of standards are the TGS Standard 1, TGS Standard 2, TGS Standard 2a, TGS Standard 3, TGS Standard 4, TGS Standard 5, TGS Equipment Spread sheet 2.

3. Existing Inventories for European Security Standards and Certification Schemes

3.1. Security standards from European Standardisation Organisations (ESOs)

European standardisation is a key instrument for the consolidation of the single market and for strengthening the competitiveness of European companies, thereby creating the conditions for economic growth. Standardisation in the EU contributes" in a significant way to the functioning of the single market, the protection of health and safety, the competitiveness of industry and the promotion of international trade, and has been supporting an increasing range of community policies". International collaborations taking place under the Dresden and Vienna Agreements. The European Security Research and Innovation Agenda [ESRIA, COM (2009)] is the final result of the two-year analysis carried out by ESRIF on security challenges facing Europe. ESRIA sets out policy and operational recommendations for achieving stronger security research and innovation results. The Communication COM (2009), 21 December 2009, "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations" essentially summarized the ESRIF report and the ESRIA proposal. The **Stockholm Programme,** adopted by the European Council in December 2009, provides a roadmap for EU work in the area of justice, freedom and security for the period 2010-14. The Programme invites the Council and Commission to develop the **Internal Security Strategy (ISS)**, with a vision of improving the protection of citizens and the fight against organized crime and terrorism by ensuring that the strategy's priorities *'are tailored to the real needs of users and focus on improving interoperability'.*

The need for a more harmonized European framework to enhance the competitiveness of the EU security industry was concluded by the *Research for a Secure Europe (2004)* and the 2009 ECORYS126 and 2011 ECORYS127 studies on security competitiveness and regulation. More harmonized European regulatory frameworks and standards have begun to take shape in the field of security, encouraged by the development of the EU Security Industrial Policy. In particular, this is taking place within the CEN/CENELEC/ETSI framework under **Mandate M/487 on Security Standards** to develop a work programme for the definition of European Standards and other standardisation deliverables in the area of security (where security refers to protection against threats by terrorism, serious and organized cross-border crime, natural disasters, pandemics and major technical accidents, excluding defence and space technologies). The Action Plan for an Innovative and Completive Security Industry [COM(2012)] was communicated in July 2012 and has three particular objectives: overcoming the fragmentation of the EU security market, reducing the gap from research to market and better integration of the societal dimension. Standards complement European and national policies in many areas. On the field of security standardisation, *Mandate M/487* ushered a new phase in the area of security with a particular emphasis on cooperation with the widest range of interested groups. The process towards this mandate was characterized by crucial stages in which EU security policies have been focused. On the area of research and innovation [as reflected in the *ESRIA proposal* (2009) or the *Communication COM (2008) final*], on the area of justice, freedom and security [as reflected in the *Stockholm Programme* (2009)] or on the internal security threats [as reflected in the EU *Internal Security Strategy* (2010)], among others. In addition, many security fields are shaped by additional documents. Besides this micro view, the European Commission communicated clear perspectives on structural aspects of the future European security-related conformity assessment system. The main domains are used for security taxonomy are the security of citizens, critical infrastructure, border security and crisis management.

ESOs of importance are mainly CEN, CENELEC and ETSI, with national standardisation organisations as members. Since all three are private organisations, a co-operation between them and the EC and the European Free Trade Association has been signed[147] in order to ensure that the voluntary and consensus-driven activity of standardisation is accepted and coherent with each other, especially due to the impact on several areas of pub-lic concern such as the industry, the single market and the environment.[148] By this it has been enabled that only standards created by those three organisations are recognised as European standards (ENs). The main Technical Committees that are relative to security topics, pictured in the Table 1.

The Technical Committees of CENELEC which are relative to the security topics are:

- CLC/TC 79, Alarm systems , monitoring systems, surveillance systems, access control systems
- CLC / BTTF 133-1, Emergency purposes which are not part of alarm systems/ emergency situations
- CLC/ TC 45AX, Instrumentation, control and electrical systems of nuclear facilities

Respectively the Technical Committees of CENELEC which are relative to the security topics are:

- ESI – Electronic Signatures and Infrastructures
- SCP – Smart Card Platform
- LI – Lawful interception
- Special committee (SC) EMTEL
- ISG quantum cryptography.

In Europe a huge variety of taxonomy is followed from the ESOs, the NSBs (and/or SDOs and. The main security standardisation roadmap that developed recently is the one under the Mandate 487 (2012). Moreover, EU projects like CIPRNet (The Critical Infrastructure Preparedness and Resilience Research Network), ENISA, and others they developed their taxonomy for special security subsectors.

Table 1. CEN TCs relative to Security topics

Committee	Title
CEN/TC 164	Water supply
CEN/TC 162	Protective clothing including hand and arm protection and lifejackets
CEN/TC 278	Intelligent transport systems
CEN/TC 250	Structural Eurocodes
CLC TC 79	Alarm Systems
CEN/TC 251	Health informatics
CEN/TC 264	Air quality
CEN/TC 127	Fire safety in buildings
CEN/TC 189	Geosynthetics
CEN/TC 79	Respiratory protective devices
CEN/TC 224	Personal identification, electronic signature and cards and their related systems and operations
CEN/TC 287	Geographic Information
CEN/TC 234	Gas infrastructure
CEN/TC 346	Conservation of Cultural Heritage
CEN/TC 325	Crime prevention through building, facility and area design
CEN/TC 352	Nanotechnologies
CEN/TC 379	Project Committee - Supply Chain security
CEN/TC 384	PC Airport and aviation security services
CEN/TC 388	Perimeter Protection
CEN/TC 391	Societal and Citizen Security
CEN/CLC/TC 4	PC - Services for fire safety and security systems
CEN/TC 417	PC - Maritime and port security services

In Table 2 the main European standards in the relative security domains are presented.

4. Summarising Advantages – Future Challenges

In accordance to the literature efforts to date have been unsuccessful in removing barriers to greater harmonization. A major obstacle for the expansion of European Fire & Security Group (EFSG) is, among others, the perceived quality of other national certificates in the relevant fields, which again highlights the quality issue. The market segments in which EFSG is active are neither dominated by certificates that certify "good" quality, nor exceptional certificates that certify "excellent" quality. Several market players perceive fundamental differences between two groups of certificates in this regard: a number of certificates whose content is comparable on a high level of quality and "other European certificates". Several European countries are perceived as providers of high quality products and solutions, and there are even companies which advertise with the slogan "made in country [X]". Specific concerns exist that collaborations with providers of "other" certificates whose requirements are less advanced bear the risk of diluting the image of their own certificate. The high level of quality which is certified by their specific marks and the excellent image of their certificates have to be kept. Therefore, measures to analyse and improve the quality infrastructure in the relevant other Member States (mostly new Member States) as well as improvements of the image of the relevant certificates, are needed. Obstacles regarding mutual recognition are also caused by organizational barriers. Smaller Member States with a small number of security companies may lack advanced infrastructures to offer these companies attractive certificates. In addition, the smallness of a national security industry hinders the recognition of a certificate by foreign certification bodies and is also a barrier to building trust. Countries with few organizations responsible for certification also have problems to become partners for multinational negotiation processes. In summary, several countries face the problem of a small security industry, the absence of well-known national quality seals and the lack of foreign trust in these seals needed to enter into multinational negotiations.

Table 2. European Standards under the four security domains per relative function

Area of security	Security of the citizens	Critical infrastructure	Border security	Crisis management
Function				
Information collection storage and management to produce intelligence	CEN/TC 251 EN 15213 EN ISO 14816:2005 ETSI ES 201 671 ETSI TR 102 022-1 ETSI TS 101 331 ETSI TS 102 900 ETSI TS 103 260 FprEN ISO 22311 ITU-T X.1520	CEN/TC 251 EN 16352:2013 FprEN ISO 22311 ETSI EN 300 338 ETSI ES 201 671 ETSI TS 101 331 ETSI TS 103 260 ITU-T X.1520	CEN/TC 251 FprEN ISO 22311 ETSI EN 300 338 ETSI ES 201 671 ETSI TS 101 331	CEN/TC 251 ETSI TR 102 022-1 ETSI TS 102 900 ETSI TS 103 260 ISO 22320:2011 FprEN ISO 22311
Detect	CEN/TC 325 CLC/TC 79 EN 15213 IEC 62851-2:2014 ISO 7240 prEN 16763	CEN/TC 325 CLC/TC 79 EN 15213 EN 60671:2011 ISO 7240 ISO 7753:1987 prEN 16763	CLC/TC 79	CLC/TC 79
Locate	CLC/TC 79 EN 15213 ISO 7240-16:2007	CLC/TC 79 ETSI EN 300 338 ISO 7240-16:2007	CLC/TC 79 ETSI EN 300 338	CLC/TC 79
Track	CLC/TC 79 EN 15213	CLC/TC 79 ETSI EN 300 338	CLC/TC 79 ETSI EN 300 338	CLC/TC 79
Assess	CEN/TS 16595:2013 EN ISO 22301 FprEN ISO 22313 ISO 7240-16:2007 ITU-T X.1520	CEN/TS 16595:2013 EN 60671:2011 EN ISO 22301 FprEN ISO 22313 ISO 7240-16:2007 ISO 11311:2011 ISO 16117:2013 ISO 20858:2007 ITU-T X.1208 ITU-T X.1520		

(table continues)

Sourse: http://crispproject.eu

Table 2. European Standards under the four security domains per relative function

Identify	CLC/TC 79 EN 1332 EN 14890 EN 15213 EN ISO 14816:2005 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 EN 60671:2011 ETSI EN 300 338 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 ETSI EN 300 338 ISO/IEC 7501-2:1997 ISO/IEC 7501-3:2005 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010	
Verify	CLC/TC 79 EN 1332 EN 14890 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 ISO/IEC 7501-2:1997 ISO/IEC 7501-3:2005 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010	CLC/TC 79
Authorise	EN 1332 EN 14890 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24787:2010 ITU-T X.1082	CEN/TR 16705:2014 EN 1332 EN 14890 EN 60965:2011 ISO 9564 ISO 13491 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010 ITU-T X.1082	CEN/TR 16705:2014 EN 1332 EN 14890 ISO/IEC 7501-2:1997 ISO/IEC 7501-3:2005 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010	

(table continues)

Sourse:http://crispproject.eu

Table 2. European Standards under the four security domains per relative function

Identify	CLC/TC 79 EN 1332 EN 14890 EN 15213 EN ISO 14816:2005 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 EN 60671:2011 ETSI EN 300 338 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 ETSI EN 300 338 ISO/IEC 7501-2:1997 ISO/IEC 7501-3:2005 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010	
Verify	CLC/TC 79 EN 1332 EN 14890 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010 ITU-T X.1082	CLC/TC 79 EN 1332 EN 14890 ISO/IEC 7501-2:1997 ISO/IEC 7501-3:2005 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010	CLC/TC 79
Authorise	EN 1332 EN 14890 ISO 9564 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24787:2010 ITU-T X.1082	CEN/TR 16705:2014 EN 1332 EN 14890 EN 60965:2011 ISO 9564 ISO 13491 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010 ITU-T X.1082	CEN/TR 16705:2014 EN 1332 EN 14890 ISO/IEC 7501-2:1997 ISO/IEC 7501-3:2005 ISO/IEC 19784 ISO/IEC 19794 ISO/IEC 24713-1:2008 ISO/IEC 24713-2:2008 ISO/IEC 24713-3:2009 ISO/IEC 24787:2010	

(table continues)

Sourse:http://crispproject.eu

A solution might be a collaborative arrangement of countries with un-known seals/quality marks for security products and the creation of a new additional seal “quality in new Member States” based on European standards and managed by a specific institution allowing the entering in collaborations with organizations such as EFSG, ENISA and ESOs. Additional suggestions and recommended steps **might** include:

- Establishment of TRUST between the involved stakeholders and lobbies
- Establishment of flexibility and acceleration in standards’ production process and investigation of the “open standards” perception
- Investigation of options to offer common certification solutions for innovative products and services like those on the ICT cybersecurity subsector (e.g. Standards bodies wants standards for Internet of Things but Vendors don't care)
- Establishment of a common “security” language in European level
- Re-examination of the performance measurement techniques for projects which are funded from FP7 and H2020 in order to avoid overlapping and acting as a brake on the performance of others.

Acknowledgments

The work of this paper was conducted at the Joint Research Centre (JRC) during my mandate as SNE (seconded national expert).

I would like to show my gratitude to the CEN and its’ experts for sharing their pearls of wisdom with me during the training course of “StandarDays” that I followed the last September of 2015.

I very thank all the exceptional Expert Members of the ERNCIP Thematic Groups (RSExEf, RN, CB Water) the meetings of which I had the honor of participating as a facilitator.

I thank all the colleagues from DG JRC and ERNCIP project for their collaboration the two years of my secondment in the EC JRC IPSC G.5.

References

1. Fabiana Scapolo, Peter Churchill, Vincent Viaud, Monica Antal, Hugo Cordova, Peter De Smedt (2014). *How will standards facilitate new production systems in the context of EU innovation and competitiveness in 2025?* JRC Foresight Study-EU 2015, 328-336, doi: 10.2788/46994 (print), 10.2788/80985 (online)
2. Hein Bollens (2011): The EU Standardisation System, Acting Head of Unit European Commission, DGENTR
3. Hein Bollens (12/02/2016): Joint Initiative on Standardisation" under the EU Single Market Strategy, LinkedIn
4. Henk J. de Vries (2015): *Governance of electrotechnical standardisation in Europe*. RSM Erasmus University, Rotterdam School of Management, May 2015
5. Jakobs, K. (2008): *CT Standardisation - Co-ordinating the Diversity*.
6. Hatto, P. (2010): *Standards and Standardisation Handbook*. EC DG RIT G1
7. Poustourli, A., Paepen, J. (2015): *ESOs and ISOs TCs relevant to ERNCIP CBRNE Thematic Groups: Case Study of Radiological Nuclear Threats Thematic Group (RN TG)*. Slides of 2015 for ERNCIP Project
8. Poustourli, A. (2015): *ESOs and ISOs TCs relevant to ERNCIP CBRNE Thematic Groups*. Slides of 2015 for ERNCIP Project
9. Poustourli, A., Georgakalou, M. (2016): *Benefits, Costs and Consequences of Standards’ setting: A literature review*. 15th Annual Science Technology and Society (STS) Conference, Graz
10. Poustourli, A., Kousoulidou, M., Tsoukala, V. (2015): *Security in Urban Critical Infrastructures: Contribution of Standards for a Holistic Approach of Protection and Resilience*. Proceedings of the 14th International Conference on Environmental Science and Technology p. cest2015_01442, GLOBAL NEST, ISSN 978-960-7475-52-7, http://cest.gnest.org/cest15proceedings/public_html/papers/cest2015_01442_oral_paper.pdf
11. Poustourli, A., Ward, D., Zachariadis, A., Schimmer, M. (2015): *An Overview of European Union and United States Critical Infrastructure Protection Policies*. Proceedings of the 12th International Conference “Standardization, Protypes and Quality: A means of Balkan Countries’ Collaboration”, p. 549-557, KOCAELI UNIVERSITY FOUNDATION, ISSN 978-605-83983-0-6, Turkey
12. Poustourli, A., Ward, D., Zachariadis, A. (2015*): European Policies and Programs for the Security of Building Constructions*. Proceedings of the Construction in the 21st Century-Changing the Field Changing the Field: Recent Developments for the Future of Engineering and Construction (Thessaloniki, Greece), CITC-8, ISBN 978-0-9894623-7-2, http://www.citcglobal.com/citc-8.html
13. Poustourli, A., Kourti, N. (2014): *Standards for Critical Infrastructure Protection (CIP) - The Contribution of ERNCIP*. EURAS proceedings 2014 (Cooperation among Standardisation Organizations and the Scientific and

Academic Community) (11th International Conference “Standardisation, Prototypes and Quality: A Means of Balkan Countries’ Collaboration”), p. 181-195, EURAS Contributions to Standardisation Research, ISBN 978-38-60-73305-2, http://publications.jrc.ec.europa.eu/repository/handle/JRC91182

14. EY (2015): *Study on the implementation of the Regulation (EU) No 1025/2012 (Article 24) – European Standardisation*. EC DG IMIESMEs J4
15. EY (2015): *Independent Review of the European Standardisation System*. Final Report, March 2015.EC DG IMIESMEs J4
16. ***: *The Annual Union Work Programme for European Standardisation for 2016*. COM(2015)686final
17. ***: *The Annual Union Work Programme for European Standardisation for 2015*. COM(2014)500final
18. A strategic vision for European standards: Moving forward to enhance and accelerate the sustainable growth of the European economy by 2020. COM(2011)311final
19. ***: *CEN and CENELEC Work Programme 2016*
20. ANEC 2015. Position Paper on the Single Market strategy COM(2015)550final, SWD(2015)2012final. ANEC-SC-2015-G-025
21. ***: *EU-European atomic Energy Community, European Committee for Standardisation and the European Committee for Electrotechnical Standardisation Cooperation Agreement*. No JRC. BXL.CA. 31691-2010
22. ***: *JRC-CEN-CENELEC Cooperation Agreement*
23. Mandate M/487 (2012). *Mandate M/487 to Establish security Standards*. Final Report Phase 1 (*Analysis of the Current Security Landscape*). EC DG EI-SRD, 9 May 2012
24. Mandate M/487 (2013): *Mandate M/487 to Establish security Standards*. Final Report Phase 2 (*Proposed standardisation work programmes and road maps*). EC DG EI-SRD, 5 July 2013. Standardisation (M/487 has been accepted by the European Standards Organizations (ESOs)/ The work has been allocated to CEN/TC 391 ‘Societal and Citizen Security’ whose secretariat is provided by the Netherlands), Standardization Institute (NEN), 05-07-2013
25. Mandate M/517 (2013): *Mandate M/517 for the programming and development of horizontal service standards*. Phase 1, Final Report, February 2015. SAGS AHG, CEN
26. EXP 384 final (2010): *Standardisation for a competitive and innovative Europe: a vision for 2020*. Report of the Expert Panel for the Review of the European Standardisation System, February 2010
27. J2572/CEN: *Research Study on the benefits of linking Innovation and Standardisation*. Final report 2014 (Optimat, brodgit) from the joint projects
28. Technopolis (2013): *Study on the contribution of standardisation to innovation in European-funded research projects*. Final report, September 2013, Technopolis group
29. Technopolis (2010): *Mapping services standardisation in Europe*. Final report, November 2010, Technopolis group
30. CEN CENELEC (2016): CEN CENELEC Operating Grant proposal 2016. SA/CEN/GROW/EFTA/000/2016-01. SA/CENELEC/GROW/EFTA/000/2016-01
31. CEN CENELEC (2015): *Common Rules for Standardisation Work*. Internal Regulations Part 2 (2015)
32. CEN CENELEC (2015): *The concept of partnership with European Organisations and other stakeholders*. Guide 25, July 2015
33. CEN CENELEC (2014): *Workshop Agreements*. Guide 29, November 2014
34. CEN CENELEC (2014): *Tasks and responsibilities of the New Approach Consultants*. Guide 15, Edition 2, May 2014
35. CEN CENELEC (2015): *Better regulation through standards-guidance for policy makers*. Guide 30, Edition 1, 2015
36. CEN CENELEC (2015): *Competition law for participants in CEN CENELEC activities*. Guide 31, Edition 1, 2015
37. CEN CENELEC brochure (2015): *How to link standardisation with research projects. Advice for CEN and CENELEC Members*
38. CEN CENELEC brochure (2015): *How to link standardisation with research projects. Tips for organizing an event for researchers*
39. CEN CENELEC brochure (2015): *How to link standardisation with research projects. Information for National Contact Points (NCPs)*
40. CEN CENELEC brochure (2015): *How to link standardisation with research projects. Standards to support research and innovation*
41. CEN BOSS (CEN Business Operations Support System). Available at http://www.cen.eu/boss
42. CEN/CENELEC Internal Regulations. Part 2: *Common rules for standardization work*. (CEN-CENELEC web site, see CEN BOSS)
43. CEN/CENELEC Internal Regulations. Part 3: *Rules for the structure and drafting of CEN/CENELEC publications*. (ISO/IEC Directives – Part 2, Modified) (CEN-CENELEC web site, see CEN BOSS)

44. ISO/IEC Directives. Part 1: *Procedures for the technical work*. (ISO/IEC web site)
45. ISO/IEC Directives. Part 2: *Rules for the structure and drafting of International Standards*. (ISO/IEC web site)
46. ISO/IEC Directives. Part 1: *Consolidated ISO Supplement – Procedures specific to ISO*. (ISO web site)
47. ISO code of conduct for the technical work (ISO web site)
48. Technical Report ANEC Information Society Working Group, 2016
49. Chenard, B. (Project Officer, G4) (2014): *Policy and Research in Security EU Security Industrial Policy & Standardisation*. "*Strengthening Science-Policy-Industry links in the CBRN-E sector*", presentation EC, Brussels, 30th January 2014
50. Chenard, B. (Project Officer, G4) (2015): *Innovation and Industry for Security DG Migration and Home Affairs*. "*Standardisation activities in the security area-M/487 to establish security standard*", presentation EC Brussels, 5th May 2015
51. Loos, M., Bueno Diaz, O. (Dec 21, 2012): *Principles of European Law: Mandate Contract*. @sellier european law publishers, ISSN 1860-0905, ISBN (eBook) 978-3-86653-970-9, https://books.google.it/books?id=EG730lY-mnAC&pg=PA107&dq=mandate+487&source=gbs_toc_r&cad=3#v=onepage&q=mandate%20487&f=false)
52. Spring, M.B., Grisham, C., O'Donnell, J., Skogseid, I., Snow, A., Tarr, G., Wang P. (2016): *From Courtship Dance to Lawyering: Working with Bulldogs and Turtles*. Department of Information Science, University of Pittsburgh, Pittsburgh, PA 15260, spring+@pitt.edu. Available at http://www.sis.pitt.edu/spring/papers/improve.pdf
53. Quevauviller, P. (2015): *Strengthening cooperation in the disaster risk and crisis management sectors – Perspectives within Horizon 2020*. Innovation and Industry for Security, presentation EC DG HOME, 2015. Available at http://ec.europa.eu/echo/files/civil_protection/civil/pdfdocs/infoday2015/DG_HOME.pdf
54. Quevauviller, P. (2015): *DRS - 2015 topics*. DG Migration and Home Affairs, DG Communication Networks, Content and Technology, Brussels, 26 April 2015, presentation EC DG HOME/B/4. Available at http://ec.europa.eu/rea/pdf/sec_infoday_2015/drs_2015_infoday_wp2015_drs_.pdf
55. Quevauviller, P. (2014): *First Science-Policy-Industry meeting on CBRN-E – Introductory words*. Security Research and Industry, DG Enterprise and Industry, Brussels, 30th January 2014
56. Wurster, S., Egyedi, T.M., Hommels, A. (2013): *The Development of the Public Safety Standard TETRA: Lessons and Recommendations for Research Managers and Strategists in the Security Industry*. (8th International Conference on) Standardization and Innovation in Information Technology (SIIT), DOI: 10.1109/SIIT.2013.6774584
57. ***: *EU Data Base of Mandates*. http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction =search.detail&id=472. Accessed: 2016-04-22
58. ***: *New Approach and European standardisation in the Internal Market*. http://www.newapproach.org/. Accessed: 2016-04-22
59. ***: *Commission sets out path to digitise European industry*. http://europa.eu/rapid/press-release_IP-16-1407_en.htm, Accessed: 2016-04-22
60. http://ec.europa.eu/dgs/home-affairs/financing/fundings/pdf/research-for-security/security_research_catalogue _2014_en.pdf
61. Discussion Paper on further steps in the implementation of the CBRN-E Agenda, European Commission
62. DIRECTORATE-GENERAL HOME AFFAIRS Directorate D: *Internal security Unit* D.1: *Counter Terrorism and Crisis Management*
63. ***: *The European Agenda on Security*. COM(2015) 185 final, http://ec.europa.eu/dgs/homeaffairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
64. European Commission, Programming Mandate addressed to CEN, CENELEC, and ETSI to establish security standards, M/487, Brussels 17.02.2011
65. http://www.efsg.org/, European Fire & Security Group
66. http://crispproject.eu/, CRISP (Evaluation and Certification Schemes for Security Products)
67. https://www.enisa.europa.eu/
68. https://www.ciprnet.eu/summary.html
69. http://www.iso.org/sites/sags/)
70. http://standards.cen.eu/dyn/www/f?p=204:105:0::::
71. http://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/
72.http://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:680331,25&cs=1DEA3EB5E0 97845A11A8E4C58418A669F
73. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2015.125.01.0001.01.ENG
74. http://www.nist.gov/forensics/osac/standards-guidelines-catalog.cfm
75. https://www.cnss.gov/CNSS/issuances/TSG_Standards.cfm
76.https://id.iso.org/sp/cdcstartSSO.ping?SpSessionAuthnAdapterId=ProxySPAdapter&TargetResource=https %3A%2F%2Fid.iso.org%2Fproxy%2F%3Fcmd%3Didp-sso-

resume%26resumePath%3D%252Fidp%252FNc4R8%252FresumeSAML20%252Fidp%252FSSO.ping

77.https://login.cen.eu/idp/SSO.saml2?SAMLRequest=fZJRT8IwFIX%2FytJ31nVziA0jQXiQBIW46YMvpIwLNHbt7O1Q%2F73dhhFfeGvSc79z7mnHKCpV82njjvoZPhpAF3xVSiPvLjLSWM2NQIlciwqQu5Ln08clj8OI19Y4UxpFgikiWCeNnhmNTQU2B3uSJbw8LzNydK7mlJagQ4kmNPZAlTyBkvr975Af5XZrFLhjiGho6xHT9SovSDD3oaQWLb6Hoacpc5A6bJnQULmraZ6vwjZzTILFPCMbxkb7u6HYwT652QIbJSzaD8XtcBinbJ%2BK1MsQG1hodEK7jMQRSwfRaMCSgiU8jniSvpFgfV7xXuqd1IfrfWx7EfKHolgP%2BvCvYLEL7gVkMm4T8s7YXvR8HSt%2ByyWTVnbukIu6VrLsahn4LdvX2G18IRsoTTWmF069bc2fPHoxXxs%2F9h1MlTKfMwvCQUYYoZN%2B5P9fmPwA&RelayState=http%3A%2F%2Fcen.iso.org%2Flivelink%2Flivelink%2Fopen%2Fcentc391%2Fmain.nsf%3Fopendatabase%26login&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=QD%2FYVR0YCaB983049v%2FRomv44%2Bt9nRekCeMzUIfOTdZvYX9A6RxYa90EFklkjC1f1Gfh7CfrnT8Er1NiC3N8F5lN232G%2Bm9ozUvgAei1WhagsI8%2BgjpnZwqu%2FH9VyfKDjt2DUQ2y8HGgOZPizBFWHOL0MWdZoPaN9HrEmKiQxqI%3D