SECUR-ED
SECured URban transportation - European Demonstration

# D11.1.3 State of the Art of Security and Privacy Policies - Standardisation

| Document identification | |
|---|---|
| **Related SP / WP** | SP1 / WP11 |
| **Related Deliverable** | D11.1 |
| **Lead Participant** | International Association of Public Transport (UITP) |
| **Contributors** | THALES, MTRS3 |

| | |
|---|---|
| **Reference** | SCR-WP11-D-UIP-024-01 |
| **Dissemination Level** | PU |
| **Lead Author** | Yves Amsler<br>Mihai Barcanescu (UITP) |
| **Reviewers** | THALES, INECO, MTRS3 |

This document is issued in the frame and for the purpose of SECUR-ED project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261605.

# History

NB: a **status** is associated to each step of the document lifecycle:

- **Draft**: this version is under development by one or several partner(s);
- **Under review:** this version has been sent for review;
- **Issued**: this version of the document has been submitted to EC.

| Version | Status | Date | Author | Main Changes |
|---|---|---|---|---|
| 0.1 | Draft | | UITP | |
| | | | | |
| | | | | |
| | | | | |

# TABLE OF CONTENTS

# 1 Abstract & Purpose

## 1.1 Purpose of the document

The master deliverable D11.1 deals with the "State of the Art of Security and Privacy Policies" relevant for SECUR-ED. Knowing the fact that **legislation**, **research** and **standardisation** are the three pillars used by the European institutions to promote common policies and measures, these three topics were identified for investigation by SECUR-ED from the very beginning of the project. Due to the amount of information which has been gathered, special sections within deliverable D11.1 have been produced for each of these issues, with the present D11.1.3 being focused on "Standardisation". This "State-of-the-Art" reviewed and started screening existing standards and technical recommendations for security which might be relevant:

- for SECUR-ED as an input for the work of the partners;
- for the public transport sector (suppliers of equipment, operators, first responders, competent authorities, etc.) as references for action.

The next steps of the project shall be to continue building upon this information and to identify topics for which recommendations with a large potential for uptake by the public transport market could be proposed for future technical harmonisation/standardisation.

## 1.2 Scope of the document

The scope of D11.1.3 is "Standardisation" used as a generic word covering several categories of technical harmonisation, including official "standards".

Technical harmonisation and especially standards are strategic tools developed on a voluntary basis by the end users within a given sector to facilitate the functioning of the market and to improve the competitiveness of the sector in a global economy.

General principles have been set up by the World Trade Organisation (WTO) to develop standardisation: namely coherence, transparency, openness, consensus, voluntary application, independence from special interests and **efficiency** ('the founding principles'). All official standardisation bodies - which are presented below in chapter 4 on EU and international standardisation bodies – follow these principles.

The aim of end users is to develop to the largest extent possible consensus standards, the use of which provides a presumption of conformity to the content of the standard. However it takes time - usually between 12 months and three years - to develop a consensus standard and to go through "public review"; that is to get an agreement of the official standardisation bodies. Therefore, and especially in the fast-changing technology sectors, it may be important for end users to agree on a less formal or less supported technical solution and to publish it quickly – usually within one year - before going through the checks and balances needed to become a full "standard".

The most consensual documents are "Standards"[1], "Specifications", "Vocabulary", "Methods" (e.g. of test), "Guides" and "Codes of Practice" (CoP). They are followed by "**Drafts for**

[1] Standards numbering depends upon the standardisation body or bodies issuing them, e.g. ENxxxx for European Standardisation Bodies.

Development" (DD) "Technical Specifications" (TS) and "Technical Reports" (TR). Then come numerous other publications which can also be used for reference, such as "Workshop Agreements" (CWA: CEN Workshop Agreement sponsored by industry; IWA: International (ISO) Workshop Agreement; ITA: Industry Technical Agreement (IEC)), or "(Formal) Published Documents" (PD - for information only), "Privately Subscribed Standards" (PSD)… and others specifically produced by given bodies. Most relevant publications are presented below in chapter 4 and chapter 5.

## 1.3 Methodology

As the master document had been considered too large to sensibly contain all sections in one corpus, the authors have decided to split the deliverable into three parts, each of them dealing with one of the key subjects identified at the beginning of the research.

In this case the information has been primarily collected by UITP through data mining in the known standardisation sources. Other written sources were: EU policies and initiatives, documents of previous research projects, research projects, etc.). Finally, more information had been gathered through interaction with the SECUR-ED partners.

The review of the collected information had been done with the help of the project partners, who have indicated, to the best of their knowledge, the relevance of the identified standards for the security topics addressed by this project.

## 1.4 Structure of the document

The entire document is presented in the **first chapter** so as to rapidly familiarize any reader with the information detailed in the next pages.

A **second chapter** is dedicated to the references and acronyms supporting D11.1.3.

The **third chapter** presents the general policy and legal framework adopted by the EU in order to set in motion a stronger orientation of the European stakeholders towards standardisation initiatives. Some duplication with D11.1.2 has been introduced to facilitate the use of D11.1.3 as a stand-alone document.

All central EU and international standardisation bodies are subsequently described in **chapter four.**

**Chapter five** is dedicated to the presentation of numerous other relevant standards, guidelines and technical recommendations that have been produced by major national and international standardisation bodies, and might be relevant for the scope of the project, and for the public transport sector in general.

The standards which are not freely available have been listed in an EXCEL file presenting their numbering, date of issue, title, body in charge and potential application for the sector – based on the knowledge of SECUR-ED partners. This EXCEL file can be downloaded through the following hyperlink:

**SECUR_ED_D11_1_3_Appendix_Standardisation.xls**

The conclusions are briefly presented in **chapter six.**

**DISCLAIMER**

The contents of this document reflect the views of the author and of the contributors listed earlier who are responsible for the information presented.

All opinions expressed are personal and do not necessarily reflect the official views or policies of any SECUR-ED partner or of any European Union (EU) institution, who assume no liability for the contents or use thereof.

The document refers to the existing standards, guidelines and technical recommendations from all the major entities involved in such activities.

# 2 References

## 2.1 List of acronyms

| | |
|---|---|
| APTA | American Public Transit Association |
| ARIB | Association of Radio Industries and Businesses (Japan) |
| ATIS | Alliance for Telecommunications Industry Solutions (USA) |
| CBRN-E | Chemical, Biological, Radiological, Nuclear and high-yield Explosives |
| CB | Certification/Validation Body |
| CC | Common Criteria Arrangement |
| CCMC | CEN-CENELEC Management Centre |
| CCRA | Common Criteria Recognition Arrangement |
| CCSA | China Communications Standards Association |
| CCTV | Closed-Circuit Television |
| CEM | Common Evaluation Methodology |
| CEN | European Committee for Standardisation |
| CENELEC | European Committee for Electrotechnical Standardisation |
| CESTI | Centre d'Evaluation de la Sécurité des Systèmes d'Information |
| CoP | Code of Practice |
| CPNI | Centre for the Protection of National Infrastructure (UK) |
| CESG | National Technical Authority for Information Assurance (UK) |
| CSOC | Cyber Security Operations Centre (UK) |
| CTSA | Counter Terrorism Security Advisor (UK) |
| CWA | CEN Workshop Agreement |
| DD | Drafts for Development |
| EC | European Commission |
| ESO | European Standards Organisation |
| ESRIA | European Security Research and Innovation Agenda |
| ESRIF | European Security Research and Innovation Forum |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| HTTP | HyperText Transfer Protocol |
| ICT | Information and Communications Technology |
| IEC | International Electrotechnical Commission |
| INSPIRE | Infrastructure for Spatial Information in the European Community |
| IP | Internet Protocol |
| ISO | International Organisation for Standardisation |
| ITA | Industry Technical Agreement (IEC) |

| | |
|---|---|
| ITU | International Telecommunication Union |
| IWA | International (ISO) Workshop Agreement |
| MIL-STDs | Military Standards |
| NaCTSO | National Counter Terrorism Security Office (UK) |
| NATO | North Atlantic Treaty Organisation |
| NERC | North American Electric Reliability Corporation (USA) |
| NFC | Near Field Communication |
| NIST | National Institute for Standards and Technology (USA) |
| NSA | NATO Standardisation Agency |
| NVA | Network Video Analytics |
| NVD | Network Video Decoder |
| NVS | Network Video Storage |
| NVT | Network Video Transmitter |
| OASIS | Organisation for the Advancement of Structured Information Standards |
| OCSIA | Office of Cyber Security & Information Assurance (UK) |
| OGC | Open Geospatial Consortium |
| ONVIF | Open Network Video Interface Forum |
| PD | (Formal) Published Documents |
| PSD | Privately Subscribed Standards |
| PSIA | Physical Security Interoperability Alliance |
| REST | Representational State Transfer |
| SEISES | Systèmes Embarqués Informatisés Sûrs et Sécurisés (FR) |
| SG | Study Group |
| SOA | Service-Oriented Architecture |
| SOAP | Simple Object Access Protocol |
| STANAG | STANdardisation AGreement |
| TAI | Telebiometrics authentication infrastructure |
| TDK | Telebiometrics digital key framework |
| TTA | Telecommunications Technology Association (Korea) |
| TTC | Telecommunications Technology Committee (Japan) |
| TR | Technical Reports |
| TS | Technical Specifications |
| UITP | International Association of Public Transport |
| UML | United modeling language profiles |
| WP | Work Package or Working Party (depending on the context) |
| WSDL | Web Services Description Language |
| WTO | World Trade Organisation |
| W3C | Word Wide Web Consortium |

## 2.2 Referenced documents

Not all sources/documents listed in the text are referenced in this clause which refers to the principal sources as follows:


R[1] European Union: Communication from the Commission, *A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations*, 21 December 2009, COM(2009)691

R[2] European Union: Council of the European Union, *The European Union Counter-Terrorism Strategy*, 30 November 2005, 14469/4/05 REV4

R[3] CEN, CENELEC and ETSI, *Mandate M/487 to Establish Security Standards, Final Report Phase 1 ,* 9 May 2012

R[4] ECORYS SCS Group*, Study on the Competitiveness of the EU security industry,* 15 November 2009, Brussels

R[5] CEN website: http://www.cen.eu/cen

R[6] CENELEC website : http://www.cenelec.eu/

R[7] ETSI website : www.etsi.org/

R[8] ISO website: http://www.iso.org/iso/home.html

R[9] IEC website: http://www.iec.ch/

R[10] ITU website: http://www.itu.int/en/Pages/default.aspx

R[11] The Common Criteria website: http://www.commoncriteriaportal.org/

R[12] NATO Standardisation Agency website: http://nsa.nato.int/nsa/

R[13] ONVIF website : www.onvif.org

R[14] OASIS website : www.oasis-open.org

R[15] SPIA Alliance website : www.psialliance.org

R[16] World Wide Web Consortium website: http://www.w3.org/standards/

R[17] The Open Geospatial Consortium http://www.opengeospatial.org/

R[18] INSPIRE website http://inspire.jrc.ec.europa.eu/

R[19] APTA website http://www.apta.com/Pages/default.aspx

R[20] NIST website: http://www.nist.gov/index.html

R[21] CPNI website: http://www.cpni.gov.uk/

R[22] NERC website: http://www.nerc.com/Pages/default.aspx

# 3 General EU Framework for Standardisation

European Standardisation Organisations – ESOs - are presented in chapter 4 below. The European Commission can mandate the ESOs to develop a program and even a content of standards in given domains:

- with regard to public transport, it has been the case with Mandate M/486 for programming and standardisation addressed to the European Standardisation Bodies in the field of Urban Rail2. Phase A (programming) has been completed in 2012. No proposal has been made in the field of Security. Phase B (standardisation) is pending. The sector – represented by UITP and UNIFE through their joint Urban Rail Platform – also produced as requested by the mandate a set of "Fundamental requirements" for Urban Rail systems which are endorsed in the CEN/CENELEC guide 26.
- with regard to Security, it has been the case with M/487 Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards[3]. These bodies were given in 2011 the task – targeting all facets of **security** - to develop an overview of the existing standards for security technologies in the EU. Response to the mandate is coordinated by CEN through CEN/TC391, Societal and Citizen Security. The remit was divided into two phases. The first phase was an inventory of market/stakeholders' needs and it also produced a set of recommendations on priorities and proposals for the range of standards that will fulfil those needs (**transport** is not explicitly mentioned). The second phase under finalisation has started in January 2013 and is establishing a set of in-depth standardisation roadmaps in selected priority fields indicating interoperability standards, equipment performance standards, minimum detection standards, organisational standards in the selected sectors (e.g. crisis management, civil protection, cyber-security…) which shall be considered in the next step of SECUR-ED WP11 works.

In addition to the works of such bodies, the EU developed with regard to **security** – in order to encourage coordinated actions of Member States enhancing the EU security framework – several initiatives potentially impacting standardisation activities which produced the following strategic documents:

- the EU Counter Terrorist Strategy and Action Plan (see clause 3.1);
- a Report on standardisation in the **security** market (ESRIF/ESRIA)(see clause 3.2);
- a Report on competitiveness of the **security industry** (ECORYS) (see clause 3.3).

It has to be noted that he recommendations regarding standardisation presented in these documents are very general, and that no proposal for new standardization work items has ever been discussed with – and therefore of course ever endorsed by - end users (as for SECUR-ED sector, especially manufacturers and operators) participating in ESOs works.

[2] http://ec.europa.eu/enterprise/standards_policy/mandates/database/index.cfm?fuseaction=search.detail&id=471

[3] http://ec.europa.eu/enterprise/standards_policy/mandates/database/index.cfm?fuseaction=search.detail&id=472

## 3.1 The EU Counter-Terrorist Strategy and Action Plan

The **EU Counter-Terrorist Strategy** of 30 November 2005[4] was the continuation of the EU work started in the wake of the Madrid bombings. Its actions were centred on 4 main objectives:

- Prevention – prevent people from turning to terrorism;
- Protection – protect citizens and infrastructure and reduce the vulnerability to attack, including through improved security of borders, transport and critical infrastructure. Although the aviation and maritime sectors were seen as the main means of transport under threats, road and rail were also acknowledged as requiring enhanced security measures. Moreover, the document stated that "To support work in all of these fields, EU research and development policy including the European Commission's R&D programmes should continue to include security related research in the context of terrorism" (Point 17). Also, EU research efforts should contribute to developing methodologies for protecting crowded places and other soft targets from attacks (Point 19). Concerning the security related research, the need to encourage it was emphasized for the following reasons: it helps to provide better security solutions; if properly design focused ("privacy by design") it helps to better protect fundamental rights; and it helps to reinforce the competitiveness;
- Pursuit – pursue and investigate terrorists across borders and globally; to impede planning, travel, and communications of terrorists. Here, Point 27 mentions that one important step will be "developing and putting into practice the principle of availability of law enforcement information. In addition, the development of new IT systems [...] while safeguarding data protection, should provide improved access to those authorities responsible for internal security thereby widening the base of information at their disposal";
- Response – to manage and minimise the consequences of a terrorist attack, by improving capabilities to deal with: the aftermath; the co-ordination of the response; and the needs of victims.

The EU proposed to address these problems through a number of measures, the most important being:

- strengthening national capabilities - Using best practice, and sharing knowledge and experiences in order to improve national capabilities to prevent, protect against, pursue and respond to terrorism, including through improved collection and analysis of information and intelligence;
- facilitating EU cooperation - Working together to share information securely between Member States and Institutions; establishing and evaluating mechanisms to facilitate cooperation including between police and judicial authorities, through legislation where necessary and appropriate.

This initiative was completed by a detailed **Action Plan** (29 March 2007)[5]. Starting from the directions outlined by the Strategy, the EU and the EMS tried to implement a set of measures

[4] http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf

[5] http://register.consilium.europa.eu/pdf/en/07/st07/st07233-re01.en07.pdf

that would reinforce the EU and national legal and political frameworks with a view of combating terrorism.

### 3.1.1 Protection

Under the Protection pillar, the FP projects are also seen as an efficient tool in overcoming market fragmentation and ensuring the establishment of better **standardisation** and certification procedures.

### 3.1.2 Respond

The "Respond" pillar is also relevant for this research, since it comprises a number of actions within the scope of D11.1.3. Under the research headlines, FP7 includes security as one of the research themes in order to develop the technologies and knowledge for building capabilities needed to guarantee the security of citizens against threats related risks such as terrorism and crime. It benefits from a budget of €1.4 billion for 2007-2013.

From what can be understood - taking a European Commission perspective - the EC put emphasis on security-related research focusing on security products because unlike the military domain, security does not have a tradition of forward planning for its future requirements from technology; due to its different nature, the market for internal security products in Europe remains highly fragmented; it would therefore help create a stronger European security industry if a dialogue on future technology needs in the field of internal security could be developed and expanded. The European Security Research and Innovation Forum (ESRIF)[6] was consequently set up in order to deliver a combined perspective of the EU security industry from various public and private stakeholders alike. This was done through the EU Security Research and Innovation Agenda (ESRIA).

## 3.2 ESRIF/ESRIA Report (2009) [7]

Based upon the ESRIF works, and with a far larger scope than standardisation the **ESRIA Report** highlighted the importance of an integrated approach to security in order to embrace, among others, interoperability, standardisation, certification, validation and the exchange of best practices.

On this basis, the European Commission intends to promote the development of a technical specification programme in the security domain which may apply to the transport sector. However the particular features of urban public transport do not support the concept and application of comprehensive mandatory specifications, particularly for operational aspects, and a voluntary approach to application is the preferred option.

The European Security Research and Innovation Forum (ESRIF) was set up in 2007 following a proposal from the EC, and is a forum for the development of a public-private

[6] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/security-research/index_en.htm

[7] Note: most of the information provided hereinafter with regard to the ESRIF Report comes from the annex of the Phase 1 report produced under the EC Programming Mandate M/487 in the field of Security:
ftp://ftp.cen.eu/CEN/Sectors/List/SecurityandDefence/SecurityoftheCitizen/M487Phase1_report.pdf

dialogue in the area of EU security research and innovation[8]. Its broader tasks are to present mid- and long-term priorities for security research through:

- bringing together all the relevant stakeholders in order to discuss issues of cross-cutting, common concern;
- identifying proposals for forming a strategic security research and innovation agenda, involving national and European stakeholders, laying out a shared and clear view of European security research needs and priorities;
- sharing ideas, views and best practices in order to make better use of existing capabilities and to enhance the use of technology in security-related domains, e.g. by inter alia making the best possible use of the various funding instruments in the present financial programming period.

By ensuring the connection between security research and security policy making, the mission of ESRIF is to support effective policies and ultimately better security to EU citizens.

It is made up of all stakeholders in security research, from the public and private sectors, i.e. industry, research establishments, public and private end-users, civil society organisations, European institutions, in particular the European Parliament, and European organisations

In particular, the ESRIF agenda is intended to establish perspectives until 2030 as well as to develop the 'innovation' dimension taking into account Member States' research activities. It promotes a more harmonised approach between security, research and innovation. In Europe's fragmented security market, standardisation can contribute to building more harmonisation to improve the region's position on the world market. Thus, ESRIF strongly supports all efforts to identify new standards and their development. The report puts forward recommendations regarding new policy initiatives, integrated approach to security and the global dimension.

The ESRIF proposed a European Security Research and Innovation Agenda (ESRIA), which is a strategic plan for security research and innovation over the next 20 years. Standardisation activities are mentioned throughout the agenda. The next table shows the systemic needs, **categorised into each of the security areas defined in the mandate, except one: "Border Security"**, which has been regarded as not relevant for the SECUR-ED project.

| Security area | Systemic needs |
|---|---|
| Security of the Citizens & Security of Infrastructures and Utilities | • Analysis of the standardisation needs in the various segments of the security market.<br>• Promotion of dynamic standardisation.<br>• Rules and integrity standards for a higher transparency of financial systems. |
| Restoring Security and Safety in Case of Crisis | • Standardisation of rescuer identity, skills and credential for interoperable command and control cooperation, for a more efficient international cooperation. |
| Others - Identity management and protection (ICT) | • Develop interoperability requirements (architectural, technical, operational etc.), aiming at agreed processes and standards. |

[8] http://europa.eu/rapid/press-release_MEMO-07-346_en.htm#PR_metaPressRelease_bottom

In Europe's fragmented security market, standardisation can contribute to building more harmonisation to improve the region's position on the world market. Thus, ESRIF strongly supports all efforts to identify necessary new standards and their development.

ESRIF has put forward a list of policy and operational recommendations, of which the following regard standardisation activities.

| Area | Recommendation |
|---|---|
| Regarding new policy initiatives | New initiatives and programmes should include the early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place. |
| Regarding integrated approach to security | Effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields. |
| Regarding the global dimension | The globally inter-related nature of security calls for giving high priority to security's external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards. |

In addition, ESRIF has also defined a roadmap. Standardisation is mentioned in the following table.

| What? | Why? | How? |
|---|---|---|
| **SECURITY OF THE CITIZEN** | | |
| Enhanced resilience and protection of the financial and payment systems | The fraud targeting the financial and payment systems is growing dramatically. New kinds of approaches are needed to address this major problem. | Rules and integrity standards for a higher transparency of financial systems. |
| Analysis of forensic traces | Analysing evidence on a crime scene is the basis of the forensic approach. This evidence is, most of the time, composed of various kinds of traces which require sophisticated tools for analysis. | International standards for trace recovery. |
| **CRISIS MANAGEMENT** | | |
| Strengthening response forces | Response forces need state-of-the-art technical equipment in the field of sensors, communications | Provide standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation |

| | | |
|---|---|---|
| | and utilities. However, the most promising way to strengthen and enforcing crisis response forces is to bundle and deepen all efforts on European level, in the Member States and by the private sector in the broad area of education, training and exercises. | for a more efficient international cooperation.<br>Address the use of virtual live exercises and other simulation-supported training methods, in particular multi-hazards training simulators, the development of appropriate and sufficient methods and tools for structured ways of lessons learned analysis, exchange and integration into planning and training, and on the education side the development of international degree courses and standards for crisis management leaders aimed at excellence would be recommended. |
| **CBRN** | | |
| CBRN integral threat assessment: Surveillance tools for detection of offensive capacity with emphasis on emerging technologies with dual-use potential; analysing actor intention; Intelligent agent data-base and sharing capabilities with high level of standardisation using validated accepted data; Systematic identification of vulnerable targets | Before prevention or preparation strategies can be applied, a complete and accurate assessment of the CBRN threat is required. Continuous assessments and foresight then helps to ascertain the efficacy of prevention strategies and future investments. An accurate CBRN threat assessment is also important to first responders and other crisis management personnel for setting planning and training agenda and can help prioritize research in this critical security area as well. | Map, through multidiscipline approaches, relevant potential pathways to CBRN terrorism (including radicalisation mechanisms in a CBRN context) and their unique and specific signatures, sensitive to group dynamics and technological abilities. Through cautious awareness raising-dialogue gain support from civil society, law enforcement, academia etc. to detect anomalies.<br>Meta-analysis of the complex threat dilemma and development of new, non-frequentist and non deterministic analysis methods.<br>Methodology to derive the probability of successful incidents. Input is from actor profiles, actor capabilities, consequence prediction, probabilistic.<br>Intelligent database development and analysis. Objective,quantitative algorithms.<br>Modelling capabilities for attack simulation and intervention planning (in/out-door; urban, sub-urban, rural, industrial infrastructure). |
| **IDENTIFICATION OF PEOPLE AND ASSETS** | | |
| Protection against Identity theft and frauds in both | Identity theft is a major current problem in the world, | Development of agreed processes and standards. |

| | | |
|---|---|---|
| physical and virtual worlds | impacting millions of people and undermining global and financial security. No coherent approach to address this threat is currently in place. It requires a concerted effort involving significant advances in processes and technology. | |
| Identification of victims during disasters and emergency Management | In case of disaster, it is critical to identify, as soon as possible the identity of the victims (including survivors). In case of major disasters, experience (2004 tsunami, Katrina) has shown that more solid and efficient solutions are needed for the management and tracking of the survivors. Solid identifications solutions, adapted to the specific context must be developed. | Standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation. |
| **INNOVATION ISSUES** | | |
| Standards development | The European security market is highly fragmented, favouring the development of multiple and incompatible solutions. A solid standardisation effort at European level would help promote the development of innovative solutions addressing the overall market, and would strengthen the European industry. | Analysis of the standardisation needs in the various segments of the security market.<br>Analysis of the conditions allowing the definition and implementation of a European Security Label.<br>Analysis of the economical impact.<br>Promotion of dynamic standardisation. |
| **GOVERNANCE AND COORDINATION** | | |
| Standardisation and Certification within a European reference system, co-ordinated by the EU and implemented through national bodies | A multitude of protection levels and standards across EU Member States increases costs for businesses, which have to incur redundant security investments depending on the jurisdictions under which they operate. The EU must define a security standard notably for strategic infrastructures. | The “Stable Structure” should be in charge of the development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability and/or commonality that are necessary to attain the required level of interoperability. |

Summarizing the above, the following list provides an overview of the standardisation activities recommended by this report in the security areas defined in the mandate:

Security of the citizen:

- fraud; standards for higher transparency of financial systems;
- identity theft and frauds (physical and virtual worlds);
- forensic traces; standards for trace recovery;
- CBRN integral threat assessment; standards for sharing capabilities.

Restoring security and safety in case of crisis:

- identification of victims; standards for rescuer identity, skills and credential to allow interoperable command and control cooperation;
- education, exercise and training; standards for crisis management leaders.

## 3.3 ECORYS Report (2009) – Study on Competitiveness of the EU Security Industry

In the study delivered by ECORYS (2009) on the Competitiveness of the European Security Industry[9] recommendations were made about the development of new European and common international standards for security (especially technical and performance standards) as a solution to reduce the Security market fragmentation, which is leading to a lack of competitiveness of the European security industry.

Given the target and importance of these documents, the available information could be considered for application in the demonstrations and after the end of the project.

9 http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf

# 4 EU and International Standardisation Bodies

European standardisation is organised by and for the stakeholders concerned based on:

- national representation – in the case of the European Committee for Standardisation (CEN) and the European Committee for Electrotehnical Standardisation (CENELEC);
- direct participation, in the case of ETSI (the European Telecommunications Standards Institute).

Directive 98/34/EC[10] officially recognised **CEN, CENELEC and ETSI** as the three European Standards Organisations (ESOs) in charge of the planning, drafting and adoption of European Standards in all areas of economic activity. This directive has been amended in November 2013 by the new EU Regulation on European Standardisation 1025/2012[11], providing the legal framework within which the ESOs operate as from 1 January 2013 (and introducing new specific provisions in the field of Information Technologies and Telecommunications).

**The International Organisation for Standardisation (ISO)[12], the International Electrotechnical Commission (IEC)[13] and the International Telecommunication Union (ITU)[14]** are the three global sister organisations that develop International Standards on similar basis.

**CEN, CENELEC, ETSI, ISO, IEC and ITU produce standards which are public, and which in the majority of cases have to be purchased to be available**. UITP has reviewed the references and titles of such security standards potentially relevant for Public Transportation. They are presented in an EXCEL file (already mentioned above in clause 1.4) which can be downloaded through the following hyperlink:

**SECUR_ED_D11_1_3_Appendix_Standardisation.xls**

ITU, as well as some other major organisations (international or national), is producing some standards, guidelines or technical recommendations which are freely available. Organisations offering such information – and the information related to security, potentially relevant for SECUR-ED – are presented in clause 4.3 below and in chapter 5.

## 4.1 CEN and CENELEC

**Since these two standardisation bodies are similar and follow the same line of activity, albeit in different sectors, they are briefly presented together.**

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0034:FR:HTML

[11] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:01:EN:HTML

[12] http://www.iso.org/iso/home.html

[13] http://www.iec.ch/

[14] http://www.itu.int/en/Pages/default.aspx

**CEN[15] is the European Committee for Standardisation.** CEN is an international non-profit association based in Brussels since 1975. It has 33 National Members (National Standardisation Bodies, NSBs) working together to develop voluntary European Standards (ENs) in all areas of economic activity with the exception of electrotechnology (CENELEC) and telecommunication (ETSI).

**CENELEC[16] is the European Committee for Electrotechnical Standardisation**. CENELEC is a non-profit technical organisation created in 1973 under Belgian law as a result of the merger of two previous European organisations: CENELCOM and CENEL. CENELEC working with National Committees (NCs) is responsible for standardisation in the electrotechnical engineering field.

The close collaboration between CEN and CENELEC was consolidated at the start of 2010 by the creation of a **common CEN-CENELEC Management Centre** (CCMC)[17] in Brussels.

**CEN and CENELEC also cooperate with respectively the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC)** to reach agreements on common standards that can be applied throughout the whole world.

The **active Technical Committees (TC) relevant to public transport security needs within CEN and CENELEC** are as follows:

- **CEN/CLC/TC 4 "Project Committee - Services for fire safety and security systems"** is a joint CEN and CENELEC Technical Committee.
- CEN/TC 79 (See below IEC/TC 79).
- **CEN/TC 224 "Biometrics" standards** mostly works internationally, in ISO/IEC JTC1/SC37, see below.
- **CEN/TC 325 "Crime prevention through building, facility and area design"** is focusing on Urban planning standards.
- **CEN/TC 379 "Project Committee - Supply Chain security"** addresses standardised crime incident reporting along the supply chain and gives advice to SMEs on how to manage and mitigate the risk of criminal and terrorist activities in the supply chain.
- **CEN/TC391 "Societal and Citizen Security"** is dedicated to enabling and improving the capability of public and private stakeholders to prepare for, respond to and recover from such destabilizing or disruptive events. **CEN/TC391 is coordinating the CEN response to Mandate M/487.**
- **CEN/TC 417 "Project Committee - Maritime and port security services"** produces standards related to the quality of service to be provided by private security companies delivering ship, port and other maritime-related security services.
- **CEN/TC 419 'Project Committee – Forensic science services'** was created in May 2012 in order to work on European Standards on forensic science services.

[15] http://www.cen.eu/cen

[16] http://www.cenelec.eu/

[17] http://www.cencenelec.eu/aboutus/MgtCentre/Pages/default.aspx

## 4.2 ETSI

**ETSI[18]- the European Telecommunications Standards Institute** - is a not-for-profit organisation with more than 700 ETSI member organisations drawn from 62 countries across the world. ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

### ETSI/3GPP / Third Generation Partnership Project[19]

**ETSI/3GPP**, the 3rd Generation Partnership Project (www.3gpp.org), is the **ETSI active body relevant to public transport security**. It is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as Organisational Partners[20]. The **current Organisational Partners are ARIB[21] (Japan), CCSA[22] (China), ETSI (Europe), ATIS[23] (USA), TTA[24] (Korea), and TTC[25] (Japan).** The establishment of 3GPP™ was formalized in December 1998 by the signing of the 'The 3rd Generation Partnership Project Agreement[26],.

The original scope of 3GPP™ was to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes). The scope was subsequently amended to include the maintenance and development of the Global System for Mobile communication (GSM™) Technical Specifications and Technical Reports including evolved radio access technologies [(e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)].

## 4.3 ISO, IEC and ITU

**ISO, IEC and ITU are the three global organisations that develop International Standards.**

**ISO[27] is the International Organisation for Standardisation** and is the world's largest developer of voluntary International Standards. Working through global consensus, it offers

[18] http://www.etsi.org/

[19] http://www.etsi.org/about/our-global-role/3gpp

[20] http://www.3gpp.org/Management/OP.htm

[21] http://www.telecomabc.com/a/arib.html

[22] http://www.ccsa.org.cn/english/

[23] http://www.atis.org/

[24] http://www.telecomabc.com/t/tta.html

[25] http://www.telecomabc.com/t/ttc.html

[26] http://www.3gpp.org/ftp/Inbox/2008_web_files/3gppagre.pdf

[27] http://www.iso.org/iso/home.html

state of the art specifications for products, services and good practice, helping to make industry more efficient and effective. It has published more than 19 000 International Standards covering almost all aspects of technology and business.

**IEC[28] is the International Electrotechnical Commission**, and the world's leading organisation for the preparation and publication of International Standards for all electrical, electronic and related technologies.

**ITU is the International Telecommunications Union,** and it brokers industry consensus on the technologies and services that form the backbone of the world's largest, most interconnected man-made system. ITU issues the world's most universally-recognized info-communications standards. Some of the standards developed by this entity are presented in the EXCEL file attached to the current report (see above page 20), while other recommendations are presented in the following section.

The active Technical Committees (TC), Joint Technical Committees (JTC), Sub-Committees (SC), Working Groups (WG), Study Groups (SG), relevant to public transport security needs within ISO, IEC and ITU are presented hereinafter first for ISO, then for joint ISO/IEC, then for IEC and finally for ITU:

## ISO

### ISO/TC 68 Financial services[29]

The scope of ISO/TC 68 is: Standardisation in the field of banking, securities and other financial services.

Total number of published ISO standards related to the TC and its SCs (number includes updates): 51.

### ISO/TC 223 Societal security[30]

The scope of ISO/TC 223 is: (Provisional) International standardisation in the area of societal security, aimed at increasing crisis management and business continuity capabilities, i.e. through improved technical, human, organisational, and functional interoperability as well as shared situational awareness, amongst all interested parties.

Total number of published ISO standards related to the TC and its SCs (number includes updates): 7.

### ISO/TC 247 Fraud countermeasures and controls[31]

[28] http://www.iec.ch/

[29] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=49650

[30] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=295786

The scope of SO/TC 247 is: Standardisation in the field of the detection, prevention and control of identity, financial, product and other forms of social and economic fraud.

Total number of published ISO standards related to the TC and its SCs (number includes updates): 1.

### ISO/IEC

### ISO/IEC JTC 1 Information technology[32]

The scope of ISO/IEC JTC 1 is: Standardisation in the field of information technology.

Total number of published ISO standards related to the TC and its SCs (number includes updates): 2611.

ISO/IEC JTC 1 has numerous Sub-Committees relevant for SECUR-ED, as follows.

### ISO/IEC JTC 1/SC 6 Telecommunications and information exchange between systems[33]

The scope of ISO/IEC JTC 1/SC 6 is: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
Number of published ISO standards under the direct responsibility of ISO/IEC JTC 1/SC 6 (number includes updates): 351.

### ISO/IEC JTC 1/SC 27 IT Security techniques[34]

The scope of ISO/IEC JTC 1/SC 27 IT is: Information technology - Security techniques - Entity authentication - Management of information and communications technology security (MICTS)
Number of published ISO standards under the direct responsibility of ISO/IEC JTC 1/SC 27 (number includes updates): 125

### ISO/IEC JTC 1/SC 37 Biometrics[35]

The scope of ISO/IEC JTC 1/SC 37 IT is all about: Information technology - Biometrics. Number of published ISO standards under the direct responsibility of ISO/IEC JTC 1/SC 37 (number includes updates): 85

---

[31] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=580925

[32] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020

[33] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45072

[34] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306

[35] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770

## IEC

### IEC/TC 79 Alarm and electronic security systems[36]

The scope of IEC/TC 79 is to prepare international standards for the protection of buildings, persons, areas and properties against fraudulent actions having the purpose to enter in a place or to take or to use something without permission and other threat related to persons.

The scope includes, but is not limited to equipment and systems, either used by ordinary persons or by trained people in the following residential and non-residential applications:

- Access control systems
- Alarm transmission systems
- Video surveillance systems
- Combined and/or integrated systems even including fire alarm systems*
- Fire detection and fire alarm systems[37]
- Intruder and hold-up alarm systems
- Remote receiving and/or surveillance centres
- Social alarm systems

These systems can be used for providing a local or remote alarm; they can be used for calling private guards, social assistance, fire brigade or police force. They can be used for recording and transmission of dated or undated information, sounds, pictures of places and people for surveillance purposes. The standards cover:

- terminology;
- technical characteristics regarding performance criteria, reliable operation, installation, maintenance;
- testing for detection, monitoring, recording, triggering an alarm and transmission to a remote centre including procedures and protocols for communication.

Electrical safety, environmental conditions and behaviour of alarm systems regarding electromagnetic compatibility are also considered with reference to the appropriate standards (e.g. Guide ISO/IEC 51).

### IEC/TC 100 Audio, video and multimedia systems and equipment[38]

The scope of IEC/TC 100 is to prepare international publications in the field of audio, video and multimedia systems and equipment. These publications mainly include specification of the performance, methods of measurement for consumer and professional equipment and their application in systems and its interoperability with other systems or equipment.

[36] http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:1269

[37] ISO/TC21/SC3 is in charge of the production of standards for "Fire detection and alarm systems"

[38] http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1297,25

Note: Multimedia is the integration of any form of audio, video, graphics, data and telecommunication and integration includes the production, storage, processing, transmission, display and reproduction of such information.

## ITU-T

### ITU-T/SG 17[39]

Work to build confidence and security in the use of information and communication technologies (ICTs) continues to intensify in a bid to facilitate more secure network infrastructure, services and applications. Over seventy standards (ITU-T Recommendations) focusing on security have been published.

ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups. Often working in cooperation with other standards development organisations and various ICT industry consortia, SG17 deals with a broad range of standardisation issues.

To give a few examples, SG17 is currently working on cyber-security; security management; security architectures and frameworks; countering spam; identity management; the protection of personally identifiable information; and the security of applications and services for the Internet of Things (IoT), smart grid, smartphones, web services, social networks, cloud computing, mobile financial systems, IPTV and telebiometrics.

Other Study Groups of ITU which are interesting to know are **ITU-T/SG 2** and **ITU-T/SG 5**

### ITU-T/SG 2[40]

Study Group 2 of ITU is home to Recommendation ITU-T E.164, the numbering standard which has played a central role in shaping the telecom networks of today. ITU-T E.164 provides the structure and functionality of telephone numbers, and without it we would not be able to communicate internationally. In recent years SG2 has worked on ENUM, an Internet Engineering Task Force (IETF) protocol for entering E.164 numbers into the Internet domain name system (DNS).

An equally important product of SG2 is Recommendation ITU-T E.212 which describes a system to identify mobile devices as they move from network to network. International mobile subscriber identity (IMSI) is a critical part of the modern mobile telecoms system, allowing the identification of a roaming mobile terminal in a foreign network and subsequently the querying of the home network for subscription and billing information.

As the world's foremost authority on international numbering, SG2 is responsible for the maintenance of ITU's International Numbering Resource (INR) database. The INR database includes repositories of the various numbers and codes overseen by ITU; a

[39] http://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

[40] http://www.itu.int/en/ITU-T/about/groups/Pages/sg02.aspx

mechanism for the exchange of administrative and operational information among administrations and private-sector players; and a channel through which ITU members can report the possible misuse of ITU-T E.164 numbers.

A recent addition to the INR database is an online database of mobile country codes (MCCs) and mobile network codes (MNCs) assigned in compliance with ITU-T E.212. MCCs and MNCs are key building blocks to IMSI, used in combination to allocate unique identities to countries' mobile telephony installations and network operators.

Study Group 2 is also responsible for standards on the management of telecom services, networks and equipment. Telecom management systems are a crucial part of the business processes at the heart of service providers' operations. Standards focus on Fault, Configuration, Accounting, Performance and Security management (FCAPS) interfaces. FCAPS interfaces sit between network elements and management systems and also between two management systems.

### ITU-T/SG 5[41]

Study Group 5 is the ITU-T Study Group responsible for studies on methodologies for evaluating the ICT effects on climate change and publishing guidelines for using ICTs in an eco-friendly way. Under its environmental mandate SG 5 is also responsible for studying design methodologies to reduce environmental effects, for example recycling of ICT facilities and equipment.

In addition to its climate focused activities the Recommendations, Handbooks and other publications produced by SG 5 have four main objectives:

- The first is to protect telecommunication equipment and installations against damage and malfunction due to electromagnetic disturbances, such as those from lightning. In this field, ITU-T SG 5 is the most experienced and competent standardisation body.
- The second is to ensure safety of personnel and users of networks against current and voltages used in telecommunication networks.
- The third is to avoid health risks from electromagnetic fields (EMF) produced by telecommunication devices and installations.
- The fourth is to guarantee a good quality of service (QoS) for high speed data services by providing requirements on characteristics of copper cables and on the coexistence of services delivered by different providers.

[41] http://www.itu.int/en/ITU-T/about/groups/Pages/sg05.aspx

# 5 Freely available Standards, Guidelines and Technical Recommendations produced by major International and National Bodies

Numerous major international and national entities have produced technical information potentially useful for SECUR-ED in the form of “standards”, guidelines or recommendations. These are publicly available on the Internet.

A number of these entities have been selected for the document, and for each of them information is provided through hyperlinks.

The International and National entities which provide security-related technical guidelines with a potential use for SECUR-ED are:

- ITU, the International Telecommunications Union;
- CC, the Common Criteria Arrangement (International partnership);
- NSA, the NATO Standardisation Agency;
- ONVIF, the Open Network Video Interface Forum;
- OASIS, the Organisation for the Advancement of Structured Information Standards;
- PSIA, the Physical Security Interoperability Alliance;
- The World Wide Web;
- REST (Representational State Transfer)/HTTP (Hypertext transfert Protocol) and Web Services\SOAP (Simple Object Access Protocol);
- OGC, the Open Geospatial Consortium, and INSPIRE, the Infrastructure for Spatial Information in the European Community;
- APTA, the American Public Transit Association;
- NIST, the National Institute for Standards and Technology (USA);
- NERC, the North American Electric Reliability Corporation (USA);
- CPNI, the Centre for the Protection of National Infrastructure (UK);
- SEISES, for Systèmes Embarqués Informatisés Sûrs et Sécurisés (FR).

Additional information available from the US Nuclear Regulatory Commission has been considered as too specific for the purpose of this study.

## 5.1 ITU Recommendations

**ITU-T Recommendations**[42] [43] are defining elements in information and communication technologies infrastructure a number of which are freely available.

The most important set of recommendations for the SECUR-ED project are those from the **ITU-T Study Group 17 – Security**.

Work on information and communication technology security continues to intensify in a bid to facilitate more secure network infrastructure, services and applications. Over 70 standards (ITU-T Recommendations) that are focusing on security have been published. Within ITU-T, Study Group 17 coordinates security-related work across all study groups. SG 17 is currently working on cyber security, identity management, telebiometrics and IPTV security. Cyber security remains high on SG 17's agenda and much work is being conducted on the exchange of cyber security information (CYBEX). Additionally, SG 17 is coordinating standardisation work covering, among others, SmartGrid security, open identity trust framework, Near Field Communication (NFC) security, etc.. SG 17 is also the place to study technical languages and description techniques. An example is the formal language Abstract Syntax Notation One (ASN.1), an important component for protocol specification or systems design. ASN.1 is used, for example, in the signaling system (SS7) for most telephone calls, package tracking, credit card verification and digital certificates, and in many of the most used software programs. Today's work is progressing towards the development of unified modeling language profiles (UML) for ITU-T languages.

The IUT-T recommendations which are regarded as relevant for SECUR-ED are listed below. The documents are freely accessible and can be downloaded by clicking on the following hyperlink: **T_REC_from_ITU.zip**

- SERIES E: Overall Network Operation, Telephone Service, Service Operation and Human Factors. Network management – International network management:
  - ITU-T E.408: Telecommunication networks security requirements;
  - ITU-T E.409: Incident organisation and security incident handling: Guidelines for telecommunication organisations.
- SERIES M: Telecommunication Management, including TMN and Network Maintenance – Telecommunications management network:
  - ITU-T M.3410: Guidelines and requirements for security management systems to support telecommunications management.
- SERIES X: Data Networks, Open System Communications and Security Information and network security – Security management:
  - ITU-T X.805 : Security architecture for systems providing end-to-end communications;
  - ITU-T X.1052: Information security management framework;
  - ITU-T X.1055: Risk management and risk profile guidelines for telecommunication organisations;

[42] http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

[43] http://www.itu.int/pub/T-REC

- ITU-T X.1056: Security incident management guidelines for telecommunications organisations;
- ITU-T X.1081: The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics;
- ITU-T X.1084: Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems;
- ITU-T X.1086: Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security;
- ITU-T X.1088: Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection;
- ITU-T X.1089: Telebiometrics authentication infrastructure (TAI) ;
- ITU-T X.1205: Overview of cyber security;
- ITU-T X.1252: Baseline identity management terms and Definitions;
- ITU-T X.1275: Guidelines on protection of personally identifiable information in the application of RFID technology;
- ITU-T X.1303: Common alerting protocol (CAP 1.1)(the current CAP 1.2 standard which has a restricted access has already been approved by OASIS[44] and has also been adopted by SECUR-ED WP[41] members);
- ITU-T X.1312: Ubiquitous sensor network middleware security Guidelines;
- ITU-T Series X Supplement 8: ITU-T X.1205 – Supplement on best practices against botnet threats.

- SERIES Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks – Internet protocol aspects – Architecture, access, network capabilities and resource management:
  - ITU-T Y.1271: Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks.

## 5.2 The Common Criteria

### *5.2.1 General presentation*

The Common Criteria (CC) is the driving force for the widest available mutual recognition of secure IT products. The web portal[45] is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

Technical recommendations which are potentially relevant for SECUR-ED are presented and accessible through hyperlinks within the text hereinafter.

[44] Organization for the Advancement of Structured Information Standards

[45] http://www.commoncriteriaportal.org/

The CC arrangement participants represent national bodies in charge of information systems security from 26 countries worldwide, among which 13 are from Europe: FR, DE, IT, NL, ES, SE, UK, AT, CZ, DK, FI, GR, HU plus two others: TR and IL

The participants (CCRA MEMBERS[46]) share the following objectives:

- to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
- to improve the availability of evaluated, security-enhanced IT products and protection profiles;
- to eliminate the burden of duplicating evaluations of IT products and protection profiles;
- to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles with:
    - Certificate authorizing schemes - http://www.commoncriteriaportal.org/ccra/schemes
    - Licensed laboratories - http://www.commoncriteriaportal.org/labs/

The purpose of this initiative is bringing about a situation in which IT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for further evaluation. It seeks to provide grounds for confidence in the reliability of the judgments on which the original certificate was based by requiring that a Certification/Validation Body (CB) issuing Common Criteria certificates should meet high and consistent standards.

The CCRA Management Committee agreed in a meeting held in Paris on 17 September 2012 on a "Vision statement for the future direction of the application of the CC and the CCRA": http://www.commoncriteriaportal.org/vision.cfm

A complete copy (in pdf format) of the Common Criteria Recognition Arrangement can be downloaded at:

http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf

### *5.2.2 Publications*

Note: The member organisations of the CCRA declare that defined assurance levels (EALs) between versions of the criteria are equivalent and can therefore be used without restrictions for composition activities.

**CC v3.1 Release 4 consists of three parts**:

| | PDF | XML |
|---|---|---|
| Part 1: Introduction and general model | CCPART1V3.1R4.pdf | CC3R3.dtd |
| | CCPART1V3.1R4_marked_changes.pdf | |

[46] http://www.commoncriteriaportal.org/ccra/members/

| | | |
|---|---|---|
| Part 2: Security functional requirements | CCPART2V3.1R4.pdf | cc3R4.XML.zip |
| | CCPART2V3.1R4_marked_changes.pdf | |
| Part 3: Security assurance requirements | CCPART3V3.1R4.pdf | |
| | CCPART3V3.1R4_marked_changes.pdf | |

**CEM v3.1 consists of one part:**

| | |
|---|---|
| CEM | CEMV3.1R4.pdf |
| | CEMV3.1R4_marked_changes.pdf |
| : | • Guide for the Transition from CC v2.3 to CC v3.1 for ADV Requirements.<br>• Transition Guide Summary of changes in the CC/CEM from v2.3 to v3.1.<br>• Guidelines for Developer Documentation according to Common Criteria Version 3.1 |

See the guides :

- http://www.commoncriteriaportal.org/cc/adv/transition_guide/
- http://www.commoncriteriaportal.org/cc/adv/transition_guide/
- http://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf

Previous versions of the CC and CEM :
http://www.commoncriteriaportal.org/cc/previous/

The following documents are CC Supporting Documents. Supporting documents are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies. They replace multiple individual interpretations and hence provide clarity for developers, evaluators, and users. Their relevance and use for particular technologies is approved by the CCRA Management Committee following submission of a suitable rationale. Their subsequent maintenance is a responsibility of the CCRA Development board.

There are two classes of CC Supporting documentation:

- Those which are termed 'Mandatory Supporting Documents' are required to have been applied when a product involving the particular technology is certified in order to support mutual recognition.
- Those which are termed 'Guidance Supporting Documents' contain more general advice.

For more information see the CCRA Procedure for Supporting Documents[47].

**Supporting Documents related to Smart Cards and similar devices**

| Document number | Document title | Class |
|---|---|---|
| 2006-06-001 | Rationale for Smart cards and similar devices | |
| CCDB-2010-03-001 | Guidance for smartcard evaluation v2.0 | Guidance |
| CCDB-2012-04-002 | Application of Attack Potential to Smartcards v2.8 | Mandatory |
| CCDB-2009-03-002 | Application of CC to Integrated Circuits v3.0 | Mandatory |
| CCDB-2009-09-001 | Requirements to perform Integrated Circuit Evaluations v1.0 | Mandatory |
| CCDB-2012-04-001 | Composite product evaluation for Smartcards and similar devices v1.2 | Mandatory |
| CCDB-2007-09-02 | ETR-template lite for composition v1.0 | Guidance |
| CCDB-2012-04-003 | Security Architecture requirements (ADV_ARC) for smart cards and similar devices | Guidance |
| CCDB-2012-04-004 | Security Architecture requirements (ADV_ARC) for smart cards and similar devices - Appendix 1 | Guidance |
| CCDB-2012-04-005 | Collection of Developer Evidence | Guidance |

**Additional CCRA Supporting Documents**

| Document Number | Title |
|---|---|
| 2002-08-009 | Reuse of Evaluation Results and Evidence |
| 2004-02-009 | Assurance Continuity |
| 2004-07-001 | Conducting Shadow Certifications |
| 2005-06-021 | Conducting Voluntary Periodic Assessments of Schemes Participating in the CCRA |
| CCDB-2006-04-004 | ST sanitising for publication |
| CCDB-2009-03-003 | Requirements to perform Integrated Circuit Evaluations |

[47] http://www.commoncriteriaportal.org/files/operatingprocedures/2006-09-003.pdf

| | |
|---|---|
| CCDB-2007-11-001 | Site Certification |

## 5.3 Other international bodies developing standards

### *5.3.1 NATO Standardisation Agency (NSA)*

NATO has also produced through its Standardisation Agency (NSA) some agreements[48] on standards (STANAG/ STANdardisation AGreement) which are relevant for SECUR-ED One of them is used as a basic reference by WP41 SECUR-ED partners dealing with CCTV: STANAG 4609 JAIS (Edition 3: 2009) on "NATO Digital Motion Imagery Standard"[49].

The standard also presents 57 Normative References and 36 Informative References issued by the Standardisation Agreements (STANAGs), Military Standards (MIL-STDs), International Telecommunication Union (ITU) and International Standards Organisation (ISO), which constitute provisions of STANAG 4609.

### *5.3.2 Open Network Video Interface Forum (ONVIF)*

Open Network Video Interface Forum (ONVIF)[50] is established as a non-profit organisation (there are currently 443 ONVIF member companies). It is an open industry forum promoting and developing global standards for interfaces of IP-based physical security products. ONVIF is committed to the adoption of IP in the security market. The ONVIF specification will ensure interoperability between products regardless of manufacturer. The cornerstones of ONVIF are:

- standardisation of communication between IP-based physical security;
- interoperability between IP-based physical security products regardless of manufacturer;
- open to all companies and organisations.

The ONVIF specification[51] defines a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF Network Interface specification defines the network device types Network Video Transmitter (NVT), Network Video Decoder (NVD), Network Video Storage (NVS) and Network Video Analytics (NVA). The specification includes detailed service requirements and interface definitions.

[48] Ratification, implementation and reservation details are available through the NSA websites (internet http://nsa.nato.int; NATO Secure WAN (http://nsa.hq.nato.int).

[49] http://www.nato.int/structur/AC/224/standard/4609/4609_documents/4609Eed03.pdf

[50] www.onvif.org

[51] http://www.onvif.org/Documents/Specifications.aspx

### 5.3.3 Organisation for the Advancement of Structured Information Standards (OASIS)

The Organisation for the Advancement of Structured Information Standards (OASIS) [52] [53] is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas. OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organisations and individual members in 100 countries. OASIS is involved in XML.org Focus Areas which are community-driven web sites devoted to specific OASIS Standards[54] and related specifications.

### 5.3.4 The Physical Security Interoperability Alliance (PSIA)

The Physical Security Interoperability Alliance (PSIA)[55] is a global consortium of more than 65 physical security manufacturers and systems integrators focused on promoting interoperability of IP-enabled security devices and systems across the security ecosystem and beyond. The PSIA promotes and develops open specifications, relevant to networked physical security technology, across all industry segments including video, storage, analytics, intrusion, and access control. PSIA supports license-free standards and specifications, which are vetted in an open and collaborative manner, to the industry as a whole. Five active working groups, IP Video, Video Analytics, Recording and Content Management, Area Control, and Systems, develop these specifications[56].

### 5.3.5 The World Wide Web (WWW)

The World Wide Web[57] is developing standards through the **World Wide Web Consortium** (W3C) made up of member organisations (379 members as of mid-April 2013) which maintain full-time staff for this purpose. W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web. They have also developed a number of standards[58].

[52] OASIS was founded under the name "SGML Open" in 1993. It began as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). The consortium changed its name to "OASIS" in 1998 to reflect an expanded scope of technical work.

[53] www.oasis-open.org

[54] https://www.oasis-open.org/standards

[55] www.psialliance.org

[56] http://www.psialliance.org/documents.html

[57] www.w3.org

[58] http://www.w3.org/standards/

### 5.3.6 REST/HTTP and Web Services\SOAP

Some high level standards have also been developed with a focus on Web services design such as REST\HTTP[59] and Web Services\SOAP[60] (related to SOA[61] approach also used in SECUR-ED).

Representational State Transfer (REST) defines a set of architectural principles by which one can design Web services that focus on a system's resources, including how resource states are addressed and transferred over HTTP[62] - Hypertext Transfer Protocol - by a wide range of clients written in different languages. REST has gained widespread acceptance across the Web as a simpler alternative to SOAP (Simple Object Access Protocol) - and Web Services Description Language (WSDL) - based Web services. Key evidence of this shift in interface design is the adoption of REST by mainstream Web 2.0 service providers—including Yahoo, Google, and Facebook—who have deprecated or passed on SOAP and WSDL-based interfaces in favour of an easier-to-use, resource-oriented model to expose their services[63].

Service-Oriented Architecture (SOA) is an IT architectural style that supports the transformation of business into a set of linked services, or repeatable business tasks that can be accessed when needed over a network[64]. This may be a local network, it may be the Internet, or it may be geographically and technologically diverse.

IBM has identified five entry points for ensuring that every SOA-based solution undertaken delivers real business value. Each entry point is coupled with a scenario, or defined approach, that implements the technologies and thus the business values defined in each entry point. Three entry points are driven by business needs: people, process, and information; and two by IT needs: connectivity and reuse entry points.

A number of standards have also been developed in relation to these technologies[65].

### 5.3.7 OGC & INSPIRE

Some international standardisation initiatives such as OGC and INSPIRE address location based standards that are widely used in information management systems.

The **Open Geospatial Consortium** (OGC) is an international industry consortium of 475 companies, government agencies and universities participating in a consensus process to develop publicly available interface standards. OGC® Standards support interoperable solutions that "geo-enable" the Web, wireless and location-based services and mainstream IT. The standards empower technology developers to make complex spatial information and services accessible and useful with all kinds of applications.

OGC® and OpenGIS® are registered trademarks of the Open Geospatial Consortium (OGC). OGC is the brand name associated with the standards and documents produced by the OGC. OGC standards are developed in a unique consensus process supported by the

---

[59] REST : Representational State Transfer; HTTP: Hypertext Transfer Protocol

[60] SOAP: Simple Object Access Protocol

[61] SOA: Service-Oriented Architecture

[62] RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1

[63] www.restpatterns.org

[64] http://www.ibm.com/developerworks/webservices/newto/

[65] http://www.ibm.com/developerworks/webservices/standards

OGC's industry, government and academic members to enable geo-processing technologies to interoperate, or "plug and play". The OGC trademark is also associated with products that implement OGC standards and that have obtained the Certified OGC Compliant brand.

In Europe a major recent development has been the entering in force of the INSPIRE Directive in May 2007, establishing an infrastructure for spatial information in Europe to support Community environmental policies, and policies or activities which may have an impact on the environment. INSPIRE is based on the **Infrastructure for Spatial Information in the European Community** established and operated by the 27 Member States of the European Union. The Directive addresses 34 spatial data themes needed for environmental applications, with key components specified through technical implementing rules. This makes INSPIRE a unique example of an EU driven legislative "regional" approach[66].

### *5.3.8 American Public Transit Association (APTA)*

APTA, the American Public Transit Association[67], is a Public Transportation association for North America which is entitled to produce standards and recommendations regarding measures to be applied by Public Transport operators. The recommendations are produced in the form of either "white paper" or "recommended practice".

APTA has been working hard in the last years in the field of Security in Public Transport. They have produced as of April 2013 a total of 36 useful documents which can be downloaded through the hyperlinks listed hereinafter.

## Control and Communications Security

APTA_RP_CCS_1_RT_001_10 Securing Control and Communications Systems in Transit Environments Part 1

## Security Emergency Management

APTA SS-SEM-S-001-08 Continuity of Operations Plan Rev 1

APTA SS-SEM-RP-002-08 Recommended Practice for First Responder Familiarization of Transit Systems

APTA SS-SEM-S-003-08 Security & Emergency Management Aspects of Special Event Service Rev 1

APTA SS-SEM-S-004-09 General Guidance on Transit Incident Drills and Exercises Rev 1

APTA SS-SEM-S-005-09 Developing a Contagious Virus Response Plan Rev 1

APTA SS-SEM-S-006-09 Shelter of Transit Vehicles and Nonrevenue Equipment During Emergencies Rev 1

APTA SEM-SS-RP-007-09 Recommended Practice: Creating an Alternate or Backup OCC

APTA SEM-SS-RP-008-09 Recommended Practice: Safe Mail and Package Handling

APTA SEM-SS-RP-009-09 Recommended Practice: Emergency Communication Strategies for Transit Agencies

APTA SS-SEM-RP-011-09 Recommended Practice: Participating in Mutual Aid

APTA SS-SEM-RP-012-09 Recommended Practice: Responding to Threat Condition Levels

[66] http://inspire.jrc.ec.europa.eu/index.cfm/pageid/2

[67] http://www.apta.com/Pages/default.aspx

APTA SS-SEM-WP-013-10 White Paper: Operational Strategies for Emergency Smoke Ventilation in Tunnels

## Security Infrastructure

APTA SS-SIS-RP-001-10 Recommended Practice for Security Lighting for Transit Passenger Facilities

APTA SS-SIS-RP-002-10 Recommended Practice for Security Lighting for Nonrevenue Transit Facilities

APTA SS-SIS-RP-003-10 Fencing Systems to Control Access to Transit Facilities

APTA SS-SIS-RP-004-10 RP: Chain Link, Mesh, or Woven Metal Fencing Systems to Control Access...

APTA SS-SIS-RP-005-10 RP: Gates to Control Access to Revenue and Nonrevenue Transit Facilities

APTA SS-SIS-RP-006-10 Ornamental Fencing Systems to Control Access at Transit Facilities

APTA SS-SIS-RP-007-10 RP: Crime Prevention Through Environmental Design (CPTED)...

APTA SS-IS-RP-008-10 Bus Stop Design and Placement Security Considerations

APTA SS-SIS-RP-009-12 Anti-Vehicle Barriers for Public Transit

APTA-SS-SIS-S-010-13Security Considerations for Public Transit

APTA-SS-SIS-RP-011-13 Security Planning for Public Transit

APTA-SS-SIS-RP-012-13 Security Operations for Public Transit

APTA-SS-SIS-RP-013-13 Physical Security for Public Transit

APTA-SS-SIS-WP-014-13 Trash and Recycling Receptacles for Transit Facilities

## Security Risk Management

APTA SS-SRM-RP-001-09, Rev. 1 RP: Security and Emergency Preparedness Plan (SEPP)

APTA SS-SRM-WP-002-10 White Paper on Random Inspections of Carry-On Items in Transit Systems

APTA SS-SRM-RP-003-09 Recommended Practice: Conducting Nonrevenue Vehicle Security Inspections

APTA SS-SRM-RP-004-11 Recommended Practice for Conducting Background Investigations

APTA SS-SRM-RP-005-12 Security Awareness Training for Transit Employees

APTA SS-SRM-RP-006-11 RP: Random Counterterrorism Measures on Transit Systems

APTA SS-SRM-007-12 Recognizing and Responding to Unattended Packages

APTA SS-SRM-RP-009-09 Recommended Practice: Identifying Suspicious Behavior in Mass Transit

APTA SS-SRM-RP-012-09 Recommended Practice: Conducting Revenue Vehicle Security Inspections

### *5.3.9 National Institute for Standards and Technology (NIST)*

NIST is the National Institute for Standards and Technology from the Technology Administration of the US Department of Commerce[68].

[68] http://www.nist.gov/index.html

**Technical recommendations issued by NIST which are potentially relevant for SECUR-ED are accessible through hyperlinks within the following text.** Resources may be helpful to the reader in scoping, planning, documenting, conducting, and evaluating IT Security exercises.

- Federal Emergency Management Agency, Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*, June 15, 2004. http://www.fema.gov/pdf/library/fpc65_0604.pdf

- Federal Information Security Management Act of 2002, *Public Law 107-347*, December 2002. http://csrc.nist.gov/policies/FISMA-final.pdf

- Homeland Security Exercise and Evaluation Program, May 2004. http://www.ojp.usdoj.gov/odp/docs/HSEEPv3.pdf

- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995. http://csrc.nist.gov/publications/nistpubs/index.html

- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. http://csrc.nist.gov/publications/nistpubs/index.html

- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. http://csrc.nist.gov/publications/nistpubs/index.html

- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. http://csrc.nist.gov/publications/nistpubs/index.html

- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003. http://csrc.nist.gov/publications/nistpubs/index.html

- NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*, February 8, 1996. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government*, October 21, 1998. http://www.fas.org/irp/offdocs/pdd/index.html

### *5.3.10 The Centre for the Protection of National Infrastructure (CPNI)*

The UK Centre for the Protection of National Infrastructure (CPNI) protects national security by providing protective security advice on physical security, personnel security and cyber security/information assurance. Protective security is “putting in place, or building into design, security measures or protocols such that threats may be deterred, detected, or the consequences of an attack minimised”.

The UK's national infrastructure is defined by the Government as: “those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends”[69].

CPNI has effective relationships with private and public sector partners, working in close collaboration with some key partners such as the police – National Counter Terrorism Security Office (NaCTSO), co-located with CPNI and the Counter Terrorism Security Advisor (CTSA) network that CPNI co-ordinates.

In response to the cyber threat, the government set up the Office of Cyber Security & Information Assurance (OCSIA) and the Cyber Security Operations Centre (CSOC) in 2010. CPNI works closely with OCSIA, CSOC and CESG (National Technical Authority for Information Assurance) in driving forward the cyber security programme for UK government and to give the UK the balance of advantage in cyberspace.

**CPNI has produced 16 Reference Documents either for first responders or regarding SCADA Cyber Security Framework and SCADA Technical Reference Documents with potential relevance to SECUR-ED as listed below**. The documents are freely accessible and can be downloaded by clicking on the following hyperlink:

CPNI_Incident_response&SCADA_Cyber_Security_Guides.zip

- 2005005-First_responders_guide
  **POLICY AND PRINCIPLES**
- 2005006-First_responders_guide_template
  **FIRST RESPONDERS’ GUIDE TEMPLATE**
- 2008031-gpg_scada_security_good_practice:
  **GOOD PRACTICE GUIDE PROCESS CONTROL AND SCADA SECURITY**
- 2008024-gpg_scada_business_risk:
  **GUIDE 1. UNDERSTAND THE BUSINESS RISK**
- 2008025-gpg_scada_implement_secure_architecture :
  **GUIDE 2. IMPLEMENT SECURE ARCHITECTURE**
- 2008026-gpg_scada_response_capabilities :
  **GUIDE 3. ESTABLISH RESPONSE CAPABILITIES**
- 2008027-gpg_scada_improve_awareness_and_skills:
  **GUIDE 4. IMPROVE AWARENESS AND SKILLS**
- 2008028-gpg_scada_manage_third_party_risk:
  **GUIDE 5. MANAGE THIRD PARTY RISK**
- 2008029-gpg_scada_engage_projects:
  **GUIDE 6. ENGAGE PROJECTS**
- 2008030-gpg_scada_establish_ongoing_governance:
  **GUIDE 7. ESTABLISH ONGOING GOVERNANCE**
- 2011mar-infosec-remote_access_for_ics
  **CPNI VIEWPOINT : CONFIGURING AND MANAGING REMOTE ACCESS FOR INDUSTRIAL CONTROL SYSTEMS**

[69] http://www.cpni.gov.uk/

- 2011may06-infosec-configuring_and_managing_remote_access_for_ics_gpg
  **CONFIGURING & MANAGING REMOTE ACCESS FOR INDUSTRIAL CONTROL SYSTEMS**
- 2011apr01-infosec-cyber_security_assessment_of_ics
  **CPNI VIEWPOINT: CYBER SECURITY ASSESSMENTS OF INDUSTRIAL CONTROL SYSTEMS**
- 2011apr28-infosec-cyber_security_assessments_of_ics_gpg
  **CYBER SECURITY ASSESSMENTS OF INDUSTRIAL CONTROL SYSTEMS A GOOD PRACTICE GUIDE**
- 2011034-securing-move-to-ip-based-networks
  **CPNI VIEWPOINT: SECURING THE MOVE TO IP-BASED SCADA/PLC NETWORKS**
- 2011034-scada-securing_the_move_to_ipbased_scada_plc_networks
  **CPNI Guide SECURING THE MOVE TO IP-BASED SCADA/PLC NETWORKS**

### *5.3.11 The North American Electric Reliability Corporation (NERC)*

Since 1968, the North American Electric Reliability Corporation (NERC) has been committed to ensuring the reliability of the bulk power system in North America.

To achieve that, NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; monitors the bulk power system; and educates, trains, and certifies industry personnel. NERC is a self-regulatory organisation, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada.

As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce reliability standards with all users, owners, and operators of the bulk power system in the United States, and made compliance with those standards mandatory and enforceable. Reliability standards are also mandatory and enforceable in Ontario and New Brunswick, and NERC is seeking to achieve comparable results in the other Canadian provinces. NERC will seek recognition in Mexico once the necessary legislation is adopted.

NERC is a non-government organisation which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.

**NERC standards with potential relevance to SECUR-ED are listed hereinafter.** The documents are freely accessible and can be downloaded by clicking on the following hyperlink: NERC_CIP_Cyber_Security_Framework.zip

- **Standard CIP-001-2a— Sabotage Reporting**
- **Standard CIP–002–4 — Cyber Security — Critical Cyber Asset Identification**
- **Standard CIP–003–4 — Cyber Security — Security Management Controls**
- **Standard CIP–004–4 — Cyber Security — Personnel and Training**
- **Standard CIP–005–4a — Cyber Security — Electronic Security Perimeter(s )**
- **Standard CIP-006-4d — Cyber Security — Physical Security**
- **Standard CIP–007–4 — Cyber Security — Systems Security Management**

- **Standard CIP–008–4 — Cyber Security — Incident Reporting and Response Planning**
- **Standard CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets**

### *5.3.12 SEISES (FR)*

**SEISES**: On-Board Safe and Secure Computerized Systems Platform (**SEISES** is an acronym in French for **S**YSTÈMES **E**MBARQUÉS **I**NFORMATISÉS, **S**ÛRS ET **S**ÉCURISÉS)

The project SEISES was defined regarding a context, challenges and needs which are specific with emphasis on computerized on-board systems, e.g. those integrated in aeronautical, space or **transport** systems or critical infrastructure. The ICT embedded in on-board systems (aerospace, vehicles, etc.) is developing at a fast pace and is bringing an increase of performance and functions allowing suppliers to extend the possibilities of competitive technical and economic solutions, but also to offer new services. The safety and security of these new services are key factors in this evolution. The SEISES project had been implemented in order to offer the relevant industries a standard that integrated safety and security alike: the terms “safety” and “security” had been chosen in order to avoid ambiguity in their understanding by the various business areas involved in the project for which the French translations may differ. These terms are used for:

- Safety: operational safety and security of goods and people
- Security: information security against malicious intent

**The SEISES consortium**

The SEISES consortium gathers the major relevant actors that can disseminate and impose these practices in their field of activity and thought their subcontractors:

- aerospace and avionics (Airbus, Thales Avionics)
- space, including launchers and vehicles (Astrium)
- communications and on-board systems (Rockwell Collins France)
- methods, techniques and technologies (APSYS, ONERA, EADS Innovation Works)
- laboratories for safety and security evaluation and certifications (CEAT, LAAS, Serma Technologies, LSTI)

The grouping of these partners is necessary to ensure the dissemination within their respective sectors as well in the standardization bodies and towards the regulatory authorities. The project coordinator is Serma Technologies Group, an expert in "safety" and "security", with transverse activities across all areas addressed by the project (aeronautics, space, automotive) which is independent as Evaluation Center of Security Information Systems (CESTI).

**Description of the SEISES Project**

SEISES is to develop a framework integrating the “safety” and “security” practices and processes within the life cycle of the on-board computerised systems, single components and related resources. This framework designed for the on-board systems is based on the Common Criteria, and gives it a practical application in this field. The project objectives are to ensure the coherence of practices and to facilitate the activities of design, development,

evaluation, validation and maintenance of safe and secure systems (including security functions).

The main goal with respect to the existing literature (ARP4761, ARP4754, DO254, DO178, ISO 15408, the Common Criteria, etc.) can be summed up with the idea to integrate security within the safety practices. SEISES also aims at completing and harmonizing the existing standards in both areas by providing a platform of integrated and tooled practices, directly applicable to the aeronautical and space domains. **The application of such practices to land transport may be done using the same model.**

This approach enables, throughout the different life-cycle phases of the on-board systems, an optimized implementation of the provisions that enable the control of hazards and threats and the management of risks, also taking into account the notion of impact (human, material, economic, image, legal and regulatory, terrorism, etc).

The following SEISES documents have been produced in French and can be downloaded by clicking the hyperlinks.

**General presentation of SISES Project**

The document provides a general view of the SEISES project: implementation background, objectives, partners and results:

http://s381942333.siteweb-initial.fr/app/download/5779572084/SEISES+-+Pr%C3%A9sentation.pdf

(Adobe Acrobat Document [1.8 MB])

**Reference guide presentation**

This document presents the reference platform resulting from SEISES project works.

http://s381942333.siteweb-initial.fr/app/download/5779572086/SEISES-Reference_guide_presentation.pdf (Adobe Acrobat Document [594.8 KB])

**Reference guide**

This document is the reference platform resulting from SEISES project works.

http://s381942333.siteweb-initial.fr/app/download/5779572087/SEISES-Reference_guide.pdf

(Adobe Acrobat Document [676.3 KB])

**Safety and Security Assurance Objective and Activity Tables**

This document is an appendix of the reference platform.

http://s381942333.siteweb-initial.fr/app/download/5779572088/SEISES_SafetySecurityTables.pdf

(Adobe Acrobat Document [369.0 KB])

**Retour des démonstrateurs SEISES (Feedback from SEISES demonstrators)**

This document presents the feedback from the three SEISES demonstrators experience : Rockwell Colins France, Thalès et Airbus

http://s381942333.siteweb-initial.fr/app/download/5779572085/Retour+d%C3%A9monstrateurs+SEISES.pdf

(Adobe Acrobat Document [1.1 MB])

# 6 Conclusions

The research done under D11.1.3 concerning standardisation related to security in the field of mass transportation (and local public transport) proved the existence of a multitude of initiatives in the security domain, at all levels – international, European and national These which have produced a tremendous amount of technical documents which are proposed by the standardisation organisations for use by the security stakeholders, and especially manufacturers and operators.

It is evident that many are already being applied to, or have implications for public transport security. At the same time bearing in mind the multitude of sources identified, it has not been possible to pinpoint comprehensively which of the identified technical documents could be of use in developing public transport security.

However Task 11.1 enabled the identification of many of them. The documents which are freely available have been listed in the present D11.1.3. The standards which have to be purchased are presented in an EXCEL File accessible through the following hyperlink:

**SECUR_ED_D11_1_3_Appendix_Standardisation.xls**

An obstacle for the further use of the latter standards - which are not dedicated to transport - is that their relevance to security in public transport depends upon the knowledge of the major partners of SECUR-ED able to cover numerous domains of applications with potential relevance to transport. Only such experts can advise on the interest of existing standards for direct application or for application after some adaptation to the public transport domain.

As part of the next task of WP11 – that is task 2 - the SECUR-ED partners will build on D11.1.3 outcomes to further conclude which existing publications are the most relevant for the sector, and whether or not additional standardisation efforts should be recommended for the public transport sector. The adoption of final recommendations is part of task 3 of WP11.

**- End of Document -**