[1]2017-08-04

Project Plan for the CEN-CENELEC Workshop on Guidelines on evaluation systems and schemes for physical security products WS Acronym: HECTOS

Workshop
(to be approved during the Kick-off meeting on 2017-08-04)

1. Status of the Project Plan

The CEN WS Hectos Project Plan was approved during kick-off meeting held in Berlin on 2017-08-04.

2. Background to the Workshop[2]

2.1 General

Physical security equipment and systems are very diverse in technology, concept of operation, application area and performance, and similar security products are difficult to compare in terms of performance, accuracy, usage, trust and validation of functionality. Currently, there are very few test, evaluation and certification procedures in Europe that are mutually recognized by different Member States. This leads to fragmentation of the market, as identified in the recent EC Communication on Security Industrial Policy, with negative impacts on both suppliers and users.

2.2. The HECTOS project

HECTOS, a project funded under the EC FP7 security research programme brings together 8 leading organizations from across Europe to study how existing evaluation and certification schemes in other areas could be used, adapted or developed for products used for physical security of people, property and infrastructure.

The HECTOS project focuses on the functional performance evaluation and conformity assessment schemes for physical security products used for security of people, property and infrastructure, including:

- Barriers (e.g. fences, gates, barriers)
- Access management (e.g. locks, safes, access control, biometrics)
- Surveillance (e.g. video surveillance systems (CCTV), security lighting)
- Detection (e.g. intruder alarms, CBRN, explosives & weapons detectors)

[1] *Here the date of updating should go, updated by the last editor*
[2] *Use font Arial 12 bold for headers (header tab stop at number 1), Arial 11 for body text*

This wide range of types of product and application, the need to operate in both regulated and unregulated environments as well as products with very different maturity and market sizes, means that a range of different types of scheme is needed. HECTOS has developed a draft of a generic scheme framework as well as a template for harmonized Evaluation and Certification schemes to accommodate these disparate needs.

The Harmonised Certification Scheme Framework for Physical Security Products developed within the HECTOS project is based on the ISO/IEC 17000 standards series for conformity assessment and adds functions and features specific for certification of security products.

2.3 Motivation for the CEN Workshop

An initial draft of the Framework has been circulated to selected stakeholders, who have shown interest in the approach. The HECTOS consortium believes that a CEN Workshop would provide an effective forum to refine and build consensus around the Framework, as well as an effective vehicle for its dissemination as a set of guidelines in a CEN Workshop Agreement. Contribution to standardization activities has been specified as one of the means for dissemination of the HECTOS project results.
The organizational structure of the project reflects this and includes a "Standardization" task where all activities related to standardization work are bundled. Results from different tasks of the project seem to be auspicious.

Comparison of performance, usage and functionality is very difficult in terms of physical security products. The Harmonised Certification Scheme Framework for Physical Security Products developed within the HECTOS project is based on the ISO/IEC 17000 standards series for conformity assessment and adds functions and features specific for certification of security products. The HECTOS framework consists of

- System key building blocks
- Scheme key building blocks
- Certification processes
- System management structure
- Certification mark hierarchy
- Actors and roles
- Controlling documents.

The framework comprises a top-level structure and a security specific ‘quality mark’; certification systems for related product and application areas; and individual certification schemes for evaluation or conformity assessment to specific standards or requirements. The objective of the framework is to provide a mechanism for the creation of harmonised evaluation and conformity assessment schemes that enable the mutual recognition between EU Member States and other

participants, thus supporting the Single Market international trade and enabling end-users better to implement security capabilities to mitigate the risks they face.

A description how to design certification schemes in the field of physical security products is missing.

For this reason the following topic has been identified as exploitable knowledge for standardization:

Guideline on designing and establishing harmonised certification systems and schemes in the field of physical security products

2.4 Market environment

The following stakeholders are considered as target groups for the use of the proposed Guideline document:

User organisations/specifiers
- End users, specifiers, advisers
- System integrators, security system designers and installers
- Service providers
- Insurers and others with a financial stake

Suppliers
- Manufacturers and distributors
- Manufacturer associations

Test and evaluation organisations
- Test houses
- Certification bodies
- Accreditation bodies

Governments and regulators
- Government organisations
- Regulators
- EC.

2.5 Existing standards and standard related activities and documents

A screening of existing standards and standardization activities has been reported within the project (in April 2016).

An overview of the identified documents can be found in Annex B.

Most of the identified standards in Annex C are related to other tasks of the HECTOS project or are just rudimentary linked to the project. However, especially the documents of ISO/IEC 17000

family (Table 1) which concur substantively with the topic of conformity assessment do not focus on a guideline how to develop a certification scheme in the field of physical security products.

The most relevant standards for the Project Plan are listed in the following Table 1:

Table 1: Most relevant standards

ISO/IEC 17000	Conformity assessment - Vocabulary and general principles
ISO/IEC 17065	Conformity assessment – Requirements for bodies certifying products, processes and services
ISO/IEC 17067	Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
ISO/IEC 17043	Conformity assessment — General requirements for proficiency testing
ISO/IEC 17011	Conformity assessment — General requirements for accreditation bodies accrediting conformity assessment bodies

CCMC and DIN secretariat will contact the CEN/CLC TC 1 for guidance allowing the evaluation of conformity of the subject of the CWA that will be duly considered during the development of the CWA content.

3. Workshop proposers and Workshop participants

Contact Point: FP 7 HECTOS (R&D project)
Coordinator contact: Anders Elfving
Department for Defence and Security, Systems and Technology
FOI Swedish Defence Research Agency
164 90 Stockholm
Sweden
Contact data: e-mail: anders.elfving@foi.se
phone: +46 8 5550 3981
http://www.hectos-fp7.eu/

The participants of the kick-off meeting will be listed in Annex A. The list of registered participants having approved the current Project Plan will be in Annex B.

4. Workshop scope and objectives

This CEN Workshop is proposed based on the scope, objectives and the outcomes of the HECTOS project, which is funded by the European Commission.

The overall goal of the envisaged CEN Workshop Agreement is to provide a guideline document how to design certification systems and schemes in the field of physical security products. Physical Security Products include products for security of people, property and infrastructure. This wide range of types of product & application, the need to operate in both regulated and unregulated environments as well as products with very different maturity and market sizes, means that a range of different types of scheme is needed. The description of a generic scheme framework to accommodate these needs is envisaged as a result of the CEN Workshop in order to transfer research results combined with stakeholder needs into standardization.

The framework, developed within HECTOS, is based on the ISO/IEC 17000 Conformity Assessment family of standards. ISO/IEC 17000 is a generic approach designed for all product types and needs to be adapted and supplemented with features to support the special requirements of security products. The proposed framework focuses on those aspects relevant for security products.

The ISO/IEC 17000 standards series is chosen in preference to the New Approach described in the EC Blue Guide which, although similar in many regards, is predicated on a model of regulated requirements derived from EU Directives. Most security products are unregulated in terms of their functional performance and the framework needs to support both voluntary and regulatory schemes.

5. Workshop programme

The deliverable of this Workshop consists of one CEN Workshop Agreement; it shall be drafted and published in English.

Work plan

Anyone can comment on this Project Plan of the envisaged CWA. All comments received will be considered by the chairperson preliminary to the kick-off meeting of participants of the Workshop where each comment received shall be presented, discussed and resolved.

Any meeting except for the kick-off can be organized as online meetings. The time schedule for the Workshop is being influenced by the runtime of the HECTOS project.

Table 2 gives an overview of the planned work schedule.

Table 2: Work plan CWA

time / activity	2017						2018	
	7	8	9	10	11	12	1	2
Public availability of project plan								
Kick-Off Meeting								
Elaboration of draft CWA								
first complete draft								
finalized draft (agreement of participants)								
Commenting Phase (public, 30days)								
Finalization of CWA, Approval of participants								
Publication								

An open commenting phase (Duration 30 days) will be considered as highly recommended as it means to enhance the transparency of the workshop process. This phase will be planned between 11/2017 and 12/2017.

6. Workshop structure

This Workshop shall be led by a chairperson and in case of absence or unavailability, by a vice-chair. The Workshop secretariat shall be responsible for the management of the Workshop.

6.1 CEN Workshop Chairperson

A proposal for the chairperson will be made by the Workshop proposers; he/she or any other candidate nominated during the period of publication of this Project Plan or at the Kick-Off will be approved at the Kick-off meeting by the parties present. His / her responsibilities include:

- Chairing the CEN Workshop meetings,
- Representing the CEN Workshop in outside meetings in cooperation with CCMC and with the Workshop secretariat,

- Monitoring the progress of the CWA,
- Interface with CCMC regarding strategic directions, problems arising, external relationships, etc.

6.2 CEN Workshop Vice-Chair

The Workshop vice-chair shall be appointed in the Kick-off meeting. The vice-chair shall support and assist in all responsibilities outlined for the chairperson. In the absence of the chairperson, the vice-chair will represent the CEN Workshop at outside meetings in cooperation with CCMC and will interface with CCMC regarding strategic directions, problems arising, external relationships etc.

6.3 CEN Workshop Secretariat

The CEN Workshop Secretariat is providing the formal link to the CEN system. The following main activities will be carried out by the Workshop Secretariat:

- Organizing CEN Workshop plenary meetings,
- Producing CEN Workshop minutes and action lists,
- Forming the administrative contact point for CWA project,
- Managing CEN Workshop attendance lists,
- Managing CEN Workshop document registers,
- Following-up action lists,
- Assisting Chairperson in monitoring and following-up of electronic discussions – in case the CEN Workshop is mainly working by electronic means,
- Administrating the liaison with relevant CEN/TCs, if applicable.

7. Resource requirements

7.1 Costs of the CEN Workshop Secretariat

The administrative costs of CEN Workshop Secretariat will be covered by resources from the FP7 project HECTOS.
The copyright of the CWA shall be with CEN.
In line with the decision of CEN/CA the possibility to download the CWA on pre-payment is covered.

7.2 Participation and Registration Fee

The registration and participation at this CEN Workshop is free of charge; each participant shall bear his/her own cost for travel and subsistence.

8. Related activities, liaisons, etc.

HECTOS is currently in liaison with CEN/TC 391 ´Societal and Citizen Security´.

9. Contact points

Such as Workshop Chairperson, Workshop Secretariat, Editors, CCMC contact, etc.

Chairperson:
Anders Elfving
FOI
Department for Defence and Security,
Systems and Technology
FOI Swedish Defence Research Agency
164 90 Stockholm
Sweden

Tel.: +46 8 5550 3981
anders.elfving@foi.se

Vice Chairperson:
Dr. Mike Kemp
Iconal Technology Ltd
St John's Innovation Centre
Cowley Road
Cambridge CB4 0WS
UK
Te..: +44 1223 313508
mike.kemp@iconal.com

CEN-CENELEC Management Centre
Alina Iatan
Programme Manager
CCMC
Avenue Marnix, 17
B-1000 Brussels
Tel.: +32 2 550 08 16
Fax: +32 2 550 08 19
aiatan@cencenelec.eu

Secretariat:
Christine Fuß
DIN
Am DIN-Platz
Burggrafenstr. 6
10787 Berlin
Germany

Tel.: +49 30 2601 2547
Fax: +49 30 2601 42547
christine.fuss@din.de
www.din.de

Annexes

Annex A List of Participants Kick-Off meeting

Annex B Participants who approve Project Plan

Annex C List of standards related to HECTOS (as found in standards research conducted in April 2016)

Annex A: List of Participants Kick-off meeting

Other interested stakeholders are welcomed to register for membership in accordance with the CEN Rules for CEN Workshops. New participants could join the WS in accordance with point 4.3.2 of CEN/CLC Guide 29 on CEN/CLC Workshop agreements expressing their interest by writing to Christine.fuss@din.de.

	Company	**Name**
1	FOI, Swedish research Agency	Anders Elfving
2	ICONAL Technology Ltd.	Mike Kemp
3	Fraunhofer ICT	Frank Schnürer
4	Fraunhofer IGD	Naser Damer
6	TNO	Clara Peters
7	SAFRAN Identity and Security	Pierre Gacon (attendance via webconference)
8	University of Warwick	Tom Sorell
9	DIN CERTCO Gesellschaft für Konformitätsbewertung mbH	Sören Scholz
10	BRE	Christopher Hunt
11	ACI-E	Thorbjörn Hennigsson
12	European Organisation for Security (EOS)	Lorraine Wilkinson, Kevin

		Riordan
13	IEC - International Electrotechnical Commission	Wolfram Zeitz
14	Euralarm	Enzo Peduzzi
15	kiwa Telfication B.V.	Henry Rutjes
16	ESSA	Ralf Demmer
17	STAC	Christophe Lagorce
18	DIN	Christine Fuß, Christopher Liedtke

Annex B: List of Participants who approve Project Plan

	Company	**Name**
1	FOI, Swedish research Agency	Anders Elfving
2	ICONAL Technology Ltd.	Mike Kemp
3	Fraunhofer ICT	Frank Schnürer
4	Fraunhofer IGD	Naser Damer
6	TNO	Clara Peters

7	SAFRAN Identity and Security	Pierre Gacon
8	University of Warwick	Tom Sorell
9	DIN CERTCO Gesellschaft für Konformitätsbewertung mbH	Sören Scholz
10	BRE	Christopher Hunt
11	ACI-E	Thorbjörn Hennigsson
12	European Organisation for Security (EOS)	Lorraine Wilkinson, Kevin Riordan
13	IEC - International Electrotechnical Commission	Wolfram Zeitz
14	Euralarm	Enzo Peduzzi
15	kiwa Telfication B.V.	Henry Rutjes
16	ESSA	Ralf Demmer
17	STAC	Christophe Lagorce

Annex C List of standards related to HECTOS (as found in standards research conducted in April 2016)

EN 12453	Industrial, commercial and garage doors and gates - Safety in use of power operated doors - Requirements
CEN/TR 16705	Perimeter protection - Performance classification methodology
CWA 16221	Vehicle security barriers - Performance requirements, test methods and guidance on application
IWA 14-1	Vehicle security barriers - Part 1: Performance requirement, vehicle impact test method and performance rating
IWA 14-2	Vehicle security barriers - Part 2: Application
BS 1722-XX series	Fences
ASTM F 2781	Standard Practice for Testing Forced Entry, Ballistic and Low Impact Resistance of Security Fence Systems
ASTM F 2656	Standard Test Method for Vehicle Crash Testing of Perimeter Barriers
SANS 301-12:2004	Fences Part 12: Specification for steel palisade fences
SANS 2220-2-7:2014*SABS 2220-2.7:2014	Electrical security systems Part 2.7: Access control systems: Barriers
LPS 1175	Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints
EN 14383-1	Prevention of crime - Urban planning and building design - Part 1: Definition of specific terms
CEN/TR 14383-2	Prevention of crime - Urban planning and building design - Part 2: Urban planning
CEN/TS 14383-3	Prevention of crime - Urban planning and building design - Part 3: Dwellings
CEN/TS 14383-4	Prevention of crime - Urban planning and design - Part 4: Shops and offices
CEN/TR 14383-5	Prevention of crime - Urban planning and building design - Part 5: Petrol stations
CEN/TR 14383-7	Prevention of crime - Urban planning and building design - Part 7: Design and management of public transport facilities
CEN/TR 14383-8	Prevention of crime - Urban planning and building design - Part 8: Protection of buildings and sites against criminal attacks with vehicles

EN 13123-1	Windows, doors and shutters - Explosion resistance; Requirements and classification - Part 1: Shock tube
EN 13123-2	Windows, doors, and shutters - Explosion resistance - Requirements and classification - Part 2: Range test
Barriers	
EN 13124-1	Windows, doors and shutters - Explosion resistance; Test method - Part 1: Shock tube
EN 13124-2	Windows, doors and shutters - Explosion resistance - Test method - Part 2: Range test
EN 356	Glass in building - Security glazing - Testing and classification of resistance against manual attack
EN 1627	Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification
EN 1628	Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Test method for the determination of resistance under static loading
EN 1629	Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Test method for the determination of resistance under dynamic loading
EN 1630	Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Test method for the determination of resistance to manual burglary attempts
EN 1522	Windows, doors, shutters and blinds – Bullet resistance - Requirements and classification
EN 1523	Windows, doors, shutters and blinds – Bullet resistance – Test method
EN 1063	Glass in building - Security glazing - Testing and classification of resistance against bullet attack
DIN 18104-1	Mechanical security equipment - Part 1: Burglar resistant products for port installation for windows and doors - Requirements and test methods
DIN 18104-2	Mechanical security devices - Part 2: Additional burglar resistant products for windows and doors - Requirements and test methods
BS 8220-series	Guide for security of buildings against crime
BS 5544	Specification for anti-bandit glazing (glazing resistant to manual attack)
BS 5357	Code of practice for installation and application of security glazing

PAS 24	Enhanced security performance requirements for doorsets and windows in the UK. External doorsets and windows intended to offer a level of security suitable for dwellings and other buildings exposed to comparable risk
NEN 5087	Burglary security of dwellings - Accessibility of roof elements and facade elements: doors, windows and frames
NEN 5096	Burglary resistance - Façade elements with doors, windows, shutters and fixed infillings - Requirements, classification and test methods
CAN/ULC-S321-M91	Standard for Burglary Resistant Vault Doors and Modular Panels
LPS 1175	Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers
LPS 1270	Requirements and testing procedures for the LPCB approval and listing of intruder resistant security glazing
Access Management	
EN 179	Building hardware. Emergency exit devices operated by a lever handle or push pad, for use on escape routes. Requirements and test methods.
EN 1125	Building hardware. Panic exit devices operated by a horizontal bar, for use on escape routes. Requirements and test methods.
EN 12209	Building hardware - Locks and latches - Mechanically operated locks, latches and locking plates - Requirements and test methods
EN 12320	Building hardware - Padlocks and padlock fittings - Requirements and test methods
EN 1300	Secure storage units - Classification for high security locks according to their resistance to unauthorized opening
EN 1303	Building hardware - Cylinders for locks - Requirements and test methods
EN 14846	Building hardware - Locks and latches - Electromechanically operated locks and striking plates - Requirements and test methods
EN 15684	Building hardware - Mechatronic cylinders - Requirements and test methods
EN 15685	Building hardware - Multipoint locks, latches and locking plates - Requirements and test methods
BS 3621	Thief resistant lock assembly. Key egress
BS 8621	Thief resistant lock assembly. Keyless egress
BS 10621	Thief resistant dual mode lock assembly.

SSF 3522 (replaced SS 3522)	Burglar-resistant locking devices for fixed mounting
SS 3620	Building hardware - Burglar resistance - Complement lockable hardware for windows and window-doors - Requirements and test methods
ABNT NBR 8208	Locks - Field testing - Method of test
ABNT NBR 8489	Locks - Laboratory testing - Method of test
ANSI/BHMA A 156.11	Cabinet Locks
ANSI/BHMA A 156.12	Interconnected Locks
ANSI/BHMA A 156.13	Mortise Locks and Latches
ANSI/BHMA A 156.2	Bored and Preassembled Locks and Latches
ANSI/BHMA A 156.23	AMERICAN NATIONAL STANDARD FOR ELECTROMAGNETIC LOCKS
ANSI/BHMA A 156.24	Delayed Egress Locking Systems
ANSI/BHMA A 156.25	Electrified Locking Devices
ANSI/BHMA A 156.28	Recommended Practices for Keying Systems
ANSI/BHMA A 156.30	High Security Cylinders
ANSI/BHMA A 156.36	Auxiliary Locks
ANSI/BHMA A 156.37	Multipoint Locks
ANSI/BHMA A 156.5	Cylinders and Input Devices for Locks
UL 437	Key locks
ASTM F 1577	Standard Test Methods for Detention Locks for Swinging Doors
ASTM F 1643	Standard Test Methods for Detention Sliding Door Locking Device Assembly
VdS 2386en	Locking Systems, Requirements and Test Methods

VdS 2396en	High Security Locks for Secure Storage Units, Requirements and Test Methods
VdS 5476en	Locking cylinders
VdS 2156-1en	Locking Cylinders with Individual Locking Function
VdS 2156-2en	Locking Cylinders with Individual Locking Function, Part 2: Electronic Locking Cylinders, Requirements and Test Methods
LPS 1142	Requirements and testing procedures
LPS 1175	Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints
EN 1143-1	Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms
EN 1143-2	Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 2: Deposit systems
EN 14450	Secure storage units - Requirements, classification and methods of test for resistance to burglary - Secure safe cabinets
EN 1300	Secure storage units - Classification for high security locks according to their resistance to unauthorized opening
EN 15659	Secure storage units - Classification and methods of test for resistance to fire - Light fire storage units
NS 5089	Safe-storage units - Testing and evaluation of burglary resistance
SFS 5320	Safe-storage units. Night safes. Testing and evaluation of burglary resistance
SSF 3492	Secure cabinet – Testing and evaluation of burglary resistance
GOST R 50862	Safes, safe rooms and strong rooms. Requirements and methods of tests for resistance to burglary and fire
UL 687	Standard for burglary resistant safes
VdS 2450	Guideline for Physical security devices - Safes, ATM safes, strongroom walls and strongroom doors - Requirements, classification and test methods
EN 60839-11-2	Alarm systems – Part 11-2:Electronic access control systems - Application guidelines
EN 50136-2	Alarm systems – Alarm transmission systems and equipment - Part 2: Requirements for Supervised Premises Transceiver (SPT)
EN 50136-3	Alarm systems - Alarm transmission systems and equipment – Part 3: Requirements for Receiving Centre Transceiver (RCT)

EN 50133-7	Alarm systems - Access control systems for use in security applications - Part 7: Application guidelines
IEC 60839-11-1	Alarm and electronic security systems – Part 11-1:Electronic access control systems - System and components requirements
	CPNI[1] Automatic Access Control Standard issue 1
	CPNI Biometric Authentication for AACS Standard
	CPNI Electronic Locking Systems Standard (electronic requirements) issue 1.1
CEN/TS 16428	Biometrics Interoperability profiles – Best Practices for slap ten print captures
CEN/TS 16634	Personal identification - Recommendations for using biometrics in European Automated Border Control
ISO/IEC 19784-1	Information technology – Biometric Application Programming Interface – Part 1: BioAPI Specification
ISO/IEC 19784-2	Information technology – Biometric Application Programming Interface – Part 2: Biometric Archive Function Provider Interface
ISO/IEC 19785-1	Information technology – Common Biometric Exchange Formats Framework (CBEFF) – Part 1: Data Element Specification
ISO/IEC 19785-2	Information technology – Common Biometric Exchange Formats Framework (CBEFF) – Part 2: Procedures for the Operation of the Biometric Registration Authority
ISO/IEC 19785-3	Information technology – Common Biometric Exchange Formats Framework (CBEFF) – Part 3: Patron format specifications
ISO/IEC 19785-4	Information technology – Common Biometric Exchange Formats Framework (CBEFF) – Part 4: Security block format specifications
ISO/IEC 24708	Information technology – Biometrics – BioAPI Interworking Protocol
ISO/IEC 19794-1	Information technology – Biometric data interchange format – Part 1: Framework
ISO/IEC 19794-2	Information technology – Biometric data interchange format – Part 2: Finger minutiae data
ISO/IEC 19794-3	Information technology – Biometric data interchange format – Part 3: Finger pattern spectral data
ISO/IEC 19794-4	Information technology – Biometric data interchange format – Part 4: Finger image data
ISO/IEC 19794-5	Information technology – Biometric data interchange format – Part 5: Face image data

ISO/IEC 19794-6	Information technology – Biometric data interchange format – Part 6: Iris image data
ISO/IEC 19794-7	Information technology – Biometric data interchange format – Part 7: Signature/sign time series data
ISO/IEC 19794-8	Information technology – Biometric data interchange format – Part 8: Finger pattern skeletal data
ISO/IEC 19794-9	Information technology – Biometric data interchange format – Part 9: Vascular image data
ISO/IEC 19794-10	Information technology – Biometric data interchange format – Part 10: Hand geometry silhouette data
ISO/IEC 19794-11	Information technology – Biometric data interchange format – Part 11: Signature/sign processed dynamic data
ISO/IEC 19794-13	Information technology – Biometric data interchange format – Part 13: Voice Data
ISO/IEC 19794-14	Information technology – Biometric data interchange format – Part 14: DNA data
ISO/IEC 19795-1	Information technology – Biometric performance testing and reporting – Part 1: Principles and framework
ISO/IEC 19795-2	Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation
ISO/IEC 19795-3	Information technology – Biometric performance testing and reporting – Part 3: Modality-specific testing
ISO/IEC 19795-4	Information technology – Biometric performance testing and reporting – Part 4: Interoperability performance testing
ISO/IEC 19795-5	Information technology – Biometric performance testing and reporting – Part 5: Access control scenario and grading scheme
ISO/IEC 19795-6	Information technology – Biometric performance testing and reporting – Part 6: Testing methodologies for operational evaluation
ISO/IEC 19795-7	Information technology – Biometric performance testing and reporting – Part 7: Testing of on-card biometric comparison algorithms
ISO/IEC 29120-1	Information technology – Machine readable test data for biometric testing and reporting – Part 1: Test reports
ISO/IEC 24709-1	Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures

ISO/IEC 24709-2	Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers
ISO/IEC 24709-3	Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 3: Test assertions for BioAPI frameworks
ISO/IEC 29109-1	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 1: Generalized conformance testing methodology
ISO/IEC 29109-2	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 2: Finger minutiae data
ISO/IEC 29109-4	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 4: Finger image data
ISO/IEC 29109-5	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 5: Face image data
ISO/IEC 29109-6	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 6: Iris image data
ISO/IEC 29109-7	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 7: Signature/sign time series data
ISO/IEC 29109-8	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 8: Finger pattern skeletal data
ISO/IEC 29109-9	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 9: Vascular image data
ISO/IEC 29109-10	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 10: Hand geometry silhouette data
ISO/IEC 29794-1	Information technology – Biometric sample quality – Part 1: Framework
ISO/IEC TR 29794-4	Information technology – Biometric sample quality – Part 4: Finger image data

ISO/IEC TR 29794-5	Information technology – Biometric sample quality – Part 5: Face image data
ISO/IEC 24713-1	Information technology – Biometric profiles for interoperability and data interchange – Part 1: Overview of biometric systems and biometric profiles
ISO/IEC 24713-2	Information technology – Biometric profiles for interoperability and data interchange – Part 2: Physical access control for employees at airports
ISO/IEC 24713-3	Information technology – Biometric profiles for interoperability and data interchange – Part 3: Biometrics-based verification and identification of seafarers
ISO/IEC TR 24722	Information technology – Biometrics – Multimodal and other multibiometric fusion
ISO/IEC 29141	Information technology – Biometrics – Tenprint capture using biometric application programming interface (BioAPI)
ISO/IEC 29144	Information technology – Biometrics – The use of biometric technology in commercial Identity Management applications and processes
ISO/IEC 29159	Information technology – Biometric calibration, augmentation and fusion data – Part 1: Fusion information format –
ISO/IEC 29164	Information technology – Biometrics – Embedded BioAPI
ISO/IEC 29195	Information technology – Biometrics – Traveller processes for biometric recognition in automated border
ISO/IEC 29197	Information technology – Biometrics – Evaluation methodology for environmental influence in biometric system performance
ISO/IEC 29198	Information technology – Biometrics – Characterization and measurement of difficulty for fingerprint databases for technology evaluation
ISO/IEC 19792	Information technology – Security techniques – Security evaluation of biometrics
ISO/IEC 24745	Information technology – Security techniques – Biometric information protection
ISO/IEC 24761	Information technology – Security techniques – Authentication context for biometrics
ISO/IEC 15408-1	Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
ISO/IEC 15408-2	Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components

ISO/IEC 15408-3	Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components
ISO/IEC 18045	Information technology – Security techniques – Methodology for IT security evaluation
TR-03121-1	Technical Guideline Biometrics for Public Sector Applications. Part 1: Framework
TR-03121-2	Technical Guideline Biometrics for Public Sector Applications. Part 2: Software Architecture
TR-03121-3	Technical Guideline Biometrics for Public Sector Applications. Part 3: Application Profiles and Function Modules, Volume 1: Verification Scenarios for ePassport and Identity Card
TR-03121 Schema	Schema and examples for BSI TR-03121
TR-03122-1	Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications, Part 1: Framework
TR-03122-2	Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications, Part 2: Software Architecture – BioAPI Conformance Testing
TR-03122-3	Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications, Part 3: Test Cases for Function Modules
Surveillance	
EN 62676-1	Video System and Transmission Requirements
EN 62676-1-1	Video System Requirements
EN 62676-1-2	Video Transmission – General Video Transmission – Requirements
EN 62676-2	Video Transmission protocols and interoperability
EN 62676-2-1	Video Transmission Protocols – General Requirements
EN 62676-2-2	Video Transmission Protocols – IP Interoperability implementation based on HTTP and REST services
EN 62676-2-3	Video Transmission Protocols – IP Interoperability implementation based on web services
EN 62676-3	Analogue and Digital Interfaces
EN 62676-4	Application Guidelines
ISO 22311	Societal Security - Video-surveillance - Export interoperability
ISO/IEC 27037	Information technology. Security techniques. Guidelines for identification, collection, acquisition, and preservation of digital evidence
IED 62676 suite	

BS 8418	Installation and remote monitoring of detector-activated CCTV systems. Code of practice
BS 8495	Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence
BS 7958	Closed circuit television (CCTV). Management and operation. Code of practice
BS 5979 – withdrawn	Remote centres receiving signals from fire and security systems. Code of practice
BS 8591	Remote centres receiving signals from alarm systems. Code of practice
UL 2044	Commercial closed-circuit television equipment
UL 3044	Surveillance closed circuit television equipment
EN 1838	Lighting applications - Emergency lighting
EN 50130-4/FprA1	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems
CEN/TS 14383-3	Prevention of crime - Urban planning and building design - Part 3: Dwellings
CEN/TS 14383-4	Prevention of crime - Urban planning and design - Part 4: Shops and offices
ISO 30061	Emergency lighting
BS 8220	Guide for security of buildings against crime
GOST R 50777	Passive infrared detectors for using at different conditions. General requirements and test methods
Detection	
EN 50130-4	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems
EN 50130-5	Alarm systems. Environmental test methods
EN 50131-1	Alarm systems - Intrusion and hold-up systems - Part 1: System requirements
EN 50131-2-2	Alarm systems - Intrusion and hold-up systems - Part 2-2: Intrusion detectors - Passive infrared detectors
EN 50131-2-3	Alarm systems – Intrusion and hold-up systems – Part 2-3: Requirements for microwave detectors

EN 50131-2-4	Alarm systems - Intrusion and hold-up-systems - Part 2-4: Requirements for combined passive infrared and microwave detectors
EN 50131-2-5	Alarm systems – Intrusion and hold-up systems – Part 2-5: Requirements for combined passive infrared and ultrasonic detectors
EN 50131-2-6	Alarm systems. Intrusion and hold-up systems Opening contacts (magnetic)
EN 50131-2-7-1	Alarm systems - Intrusion and hold-up systems - Part 2-7-1: Intrusion detectors - Glass break detectors (acoustic)
EN 50131-2-7-2	Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive)
EN 50131-2-7-3	Alarm systems - Intrusion and hold-up systems - Part 2-7-3: Intrusion detectors - Glass break detectors (active)
EN 50131-3	Alarm systems - Intrusion and hold-up systems - Part 3: Control and indicating equipment
EN 50131-4	Alarm systems - Intrusion and hold-up systems - Part 4: Warning devices
EN 50131-5-3	Alarm systems. Intrusion systems. Requirements for interconnections equipment using radio frequency techniques
EN 50131-6	Alarm systems. Intrusion and hold-up systems. Power supplies
EN 50131-8	Alarm systems - Intrusion and hold up-systems - Part 8: Security fog device/systems
EN 50131-10	Alarm systems - Intrusion and hold-up systems - Part 10: Application specific requirements for supervised premises transceiver (SPT)
EN 50131-11	Alarm systems - Intrusion and hold-up systems - Part 11: Hold-up devices
CLC/TS 50131-2-8	Alarm systems - Intrusion and hold-up systems - Part 2-8: Intrusion detectors - Shock detectors
DD CLC/TS 50131-7	Alarm systems. Intrusion and hold-up systems. Application guidelines
CLC/TS 50131-9	Alarm systems - Intrusion and hold up systems - Part 9: Alarm verification - Methods and principles
CLC/TS 50131-11	Alarm systems - Intrusion and hold-up systems - Part 11: Hold-up devices
CLC/TS 50136-7	Alarm systems - Alarm transmission systems and equipment - Part 7: Application guidelines
IEC 62642 series	Alarm Systems – Intrusion and hold-up systems
NF C48-371	Alarm systems - Combined and integrated alarm systems - General requirements

BS 8243	Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice.
BS PD 6662	Scheme for the application of European standards for intrusion and hold-up alarm systems
NIST SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
ANSI/UL 365	Standard for Safety for Police Station Connected Burglar Alarm Units and Systems
ANSI/UL 603	Standard for Safety for Power Supplies for Use with Burglar-Alarm Systems
ANSI/UL 609	Standard for Safety for Local Burglar Alarm Units and Systems
ANSI/UL 636	Standard for Safety for Holdup Alarm Units and Systems
ANSI/UL 639	Standard for Safety for Intrusion-Detection Units
ANSI/UL 681	Standard for Safety for Installation and Classification of Burglar and Holdup Alarm Systems
ANSI/UL 827	Standard for Safety for Central-Station Alarm Services
ANSI/UL 1023	Standard for Safety for Household Burglar-Alarm System Units
ANSI/UL 1037	Standard for Antitheft Alarms and Devices
ANSI/UL 1076	Standard for Safety for Proprietary Burglar Alarm Units and Systems
ANSI/UL 1610	Standard for Safety for Central-Station Burglar-Alarm Units
ANSI/UL 1635	Standard for Safety for Digital Alarm Communicator System Units
ANSI/UL 1641	Standard for Safety for Installation and Classification of Residential Burglar Alarm Systems (Proposal dated 11/7/14)
ANSI/UL 1638	Standard for Safety for Visual Signaling Appliances - Private Mode Emergency and General Utility Signaling
VdS 2195en	Class A Power Supply Units for Intruder Alarm Systems, Requirements
VdS 2227en	Intruder Alarm Systems, General Requirements and Test methods
VdS 2270en	Alarm Glasses for Intruder Alarm Systems, Requirements
VdS 2271en	Hold-up Trigger Devices for Intruder Alarm Systems, Requirements
VdS 2300en	Audible Warning Devices for External Alarm for Intruder Alarm Systems, Requirements
VdS 2301en	Visual Warning Devices for External Alarm For Intruder Alarm Systems, Requirements
VdS 2312en	Motion Detectors for Intruder Alarm Systems, Requirements and Test Methods
VdS 2332en	Glass Break Detectors for Intruder Alarm Systems, Requirements
VdS 2347en	Integrated Alarm Systems, Requirements

VdS 2465-S1en	Transmission protocol for Alarm signals/messages; Amendment S1: Correction and adaption of record types
VdS 2465-S2en	Transmission protocol for Alarm signals/messages, Amendment S2: Protocol extension for connection to networks of the TCP protocol family
VdS 2465en	Transmission protocol for Alarm Systems (AS)
ASTM E2885 -13	Standard Specification for Handheld Point Chemical Vapor Detectors (HPCVD) for Homeland Security Applications
ASTM E2933 -13	Standard Specification for Stationary Point Chemical Vapor Detectors (SPCVD) for Homeland Security Applications
ASTM E2411 -07	Standard Specification for Chemical Warfare Vapor Detector (CWVD)
ANSI N 42.41	American National Standard Minimum Performance Criteria for Active Interrogation Systems Used for Homeland Security
ASTM E 2458-10	Standard Practices for Bulk Sample Collection and Swab Sample Collection of Visible Powders Suspected of Being Biological Agents from Nonporous Surfaces
EN 60325	Radiation protection instrumentation. Alpha, beta and alpha/beta (beta energy 60 keV)
EN 60761	Equipment for continuous monitoring radioactivity in gaseous effluents
EN 60846	Radiation protection instrumentation - Ambient and/or directional dose equivalent (rate) meters and/or monitors for beta, X and gamma radiation
EN 61098	Radiation protection instrumentation - Installed personnel surface contamination monitoring assemblies
EN 61005	Radiation protection instrumentation - Neutron ambient dose equivalent (rate) meters
EN 61582	Radiation protection instrumentation. In vivo counters. Classification, general requirements and test procedures for portable, transportable and installed equipment
EN 62022	Installed monitors for the control and detection of gamma radiations contained in recyclable or non-recyclable materials transported by vehicles.
EN 62244	Radiation protection instrumentation - Installed radiation monitors for the detection of radioactive and special nuclear materials at national borders
EN 62327	Radiation protection instrumentation - Hand-held instruments for the detection and identification of radionuclides and for the indication of ambient dose equivalent rate from photon radiation.

EN 62363	Radiation protection instrumentation - Portable photon contamination meters and monitors
EN 62387	Radiation protection instrumentation. Passive integrating dosimetry systems for environmental and personal monitoring. General characteristics and performance requirements.
IEC 60325	Radiation protection instrumentation - Alpha, beta and alpha/beta (beta energy >60 keV) contamination meters and monitors
IEC 60846 series	Radiation protection instrumentation - Ambient and/or directional dose equivalent (rate) meters and/or monitors for beta, X and gamma radiation
IEC 61098	Radiation protection instrumentation - Installed personnel surface contamination monitoring assemblies
IEC 61582	Radiation protection instrumentation - In vivo counters - Classification, general requirements and test procedures for portable, transportable and installed equipment
IEC 62022	Installed monitors for the control and detection of gamma radiations contained in recyclable or non-recyclable materials transported by vehicles. *This has been adopted as the European standard EN 62022.*
IEC 62244	Radiation protection instrumentation. Installed radiation monitors for the detection of radioactive and special nuclear materials at national borders. *This is part of the corresponding European standard EN 62244.*
IEC 62327	Radiation protection instrumentation - Hand-held instruments for the detection and identification of radionuclides and for the indication of ambient dose equivalent rate from photon radiation. *This has been adopted as the corresponding European standard EN 62327*
IEC 62363	Radiation protection instrumentation - Portable photon contamination meters and monitors. *This has been adopted as the European standard EN 62363.*
IEC 62387	Radiation protection instrumentation. Passive integrating dosimetry systems for environmental and personal monitoring. General characteristics and performance requirements.
IEC 62618	Radiation protection instrumentation – Spectroscopy-based alarming Personal Radiation Detectors (SPRD) for the detection of illicit trafficking of radioactive material
IEC 62694	Radiation protection instrumentation – Backpack-type radiation detector (BRD) for the detection of illicit trafficking of radioactive material

ISO 21909-1	Passive neutron dosimetry systems. Part 1. Performance and test requirements for personal dosimetry
ISO 22188	Monitoring for inadvertent movement and illicit trafficking of radioactive material
IEEE/ANSI N 42.25	American National Standard - Calibration and usage of alpha/beta proportional counters
IEEE/ANSI N 42.28	American National Standard Calibration of Germanium Detectors for In-Situ Gamma-Ray Measurements
IEEE/ANSI N 42.35	American National Standard Evaluation and Performance of Radiation Detection Portal Monitors for Use in Homeland Security
IEEE/ANSI N 42.53	American National Standard Performance Criteria for Backpack-Based Radiation-Detection Systems Used for Homeland Security
IEEE/ANSI N 42.32	American National Standard Performance Criteria for Alarming Personal Radiation Detectors for Homeland Security
IEEE/ANSI N 42.33	American National Standard for Portable Radiation Detection Instrumentation for Homeland Security
IEEE/ANSI N 42.37	American National Standard for Training Requirements for Homeland Security Purposes Using Radiation Detection Instrumentation for Interdiction and Prevention
IEEE/ANSI N 42.43	American National Standard Performance Criteria for Mobile and Transportable Radiation Monitors Used for Homeland Security
IEEE 309/ANSI N 42.3	Test procedures and bases for Geiger-Mueller counters
ANSI N 42.34	American National Standard Performance Criteria for Handheld Instruments for the Detection and Identification for Radionuclides
ANSI N 42.38	American National Standard Performance Criteria for Spectroscopy Based Portal Monitors Used for Homeland Security
ANSI N 42.39	American National Standard for Performance Criteria for Neutron Detectors for Homeland Security
ANSI N 42.48	American National Standard Performance Requirements for Spectroscopic Personal Radiation Detectors (SPRDs) for Homeland Security
ANSI N 42.49A/B	Performance Criteria for Personal Emergency Radiation Detectors (PERDs) for Exposure Control
ANSI N 42.41	American National Standard Minimum Performance Criteria for Active Interrogation Systems Used for Homeland Security

ASTM C1169-97	Standard guide for laboratory evaluation of atomic pedestrian SNM monitor performance
Nuclear Security Series 1, IAEA, 2006	Technical and Functional Specifications for Border Monitoring Equipment
IAEA-TECDOC-1312, 20024	Detection of radioactive material at borders
IAEA-TECDOC-CD-1596	Improvement of Technical Measures to Detect and Respond to Illicit Trafficking of Nuclear and Radioactive Materials
IAEA Coordinated Research Project (CRP) (2008 – 2011)	Development and Implementation of Instruments and Methods for Detection of Unauthorized Acts Involving Nuclear and other Radioactive Material.
IEC 62463	Radiation protection instrumentation - X-ray systems for the screening of persons for security and the carrying of illicit items
IEC 62709	Radiation protection instrumentation - Security screening of humans - Measuring the imaging performance of X-ray systems
PAS 127	Checkpoint security screening of people and their belongings
NIJ 0601.03 (draft)	Walk-Through Metal Detector Standard for Public Safety
ASTM C 1269	Standard Practice for Adjusting the Operational Sensitivity Setting of In-Plant Walk-Through Metal Detectors
ASTM C 1270	Standard Practice for Detection Sensitivity Mapping of In-Plant Walk-Through Metal Detectors
ANSI N 42.44	American National Standard for the Performance of Checkpoint Cabinet X-Ray Imaging Security Systems
ANSI N 42.45	American National Standard for Evaluating the Image Quality of X-ray Computed Tomography (CT) Security-Screening Systems
ANSI N 42.47	Measuring the Imaging Performance of X-ray and Gamma-ray Systems for Security Screening of Humans
PAS 97	A specification for mail screening and security
ASTM F 792	Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems
IEEE/ANSI N 42.55	American National Standard for the Performance of Portable Transmission X-Ray Systems for Use in Improvised Explosive Device and Hazardous Device Identification.
ANSI N 42.44	American National Standard for the Performance of Checkpoint Cabinet X-Ray Imaging Security Systems

ANSI N 42.45	American National Standard for Evaluating the Image Quality of X-ray Computed Tomography (CT)Security-Screening Systems
ANSI N 42.46	Determination of the Imaging Performance of X-Ray and Gamma-Ray Systems for Cargo and Vehicle Security Screening
ASTM E 2520	Standard practice for verifying minimum acceptable performance of trace explosive detectors
ASTM E 2677	Standard test method for determining limits of detection in explosive trace detectors