CEN

WORKSHOP

AGREEMENT

CWA 17260

May 2018

ICS 13.310

English version

Guidelines on evaluation systems and schemes for physical security products

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

European foreword

This CEN-CENELEC Workshop Agreement (CWA) was discussed at the Kick-off meeting of the CEN Workshop on Guidelines on evaluation systems and schemes for physical security products.

CWA 17260:2018 was developed in accordance with CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – The way to rapid agreement" and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was agreed on 2017-08-04 in a Workshop by representatives of interested parties, approved and supported by CEN and CENELEC following a public call for participation made on 2017-07-05. It does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

The formal decision to start work on this CEN-CENELEC Workshop Agreement "Guidelines on evaluation systems and schemes for physical security products" was taken at the kick off meeting held in August 2017.

The development of this CEN-CENELEC Workshop Agreement took place in the framework of the H2020 HECTOS project.

The final text of this CWA 17260 was approved by the Workshop participants on 2018-01-28. It was developed and approved by:

— Swedish Defence Research Agency, FOI (Chair)

— Iconal Technology Ltd (Vice-Chair)

— Asociatia Romana pentru Tehnica de Securitate, ARTS

— BRE Global Ltd

— DIN CERTCO Gesellschaft für Konformitätsbewertung mbH

— European Certification Body GmbH, ECB

— European Security Systems Association e.V., ESSA

— IDEMIA

— Fraunhofer-Institut für Chemische Technologie, Fh-ICT

— Fraunhofer-Institut für Grafische Datenverarbeitung, Fh-IGD

— National Physical Laboratory, NPL

— The Netherlands Organization for Applied Scientific Research, TNO

It is possible that some elements of CWA 17260 may be subject to patent rights. The CEN-CENELEC policy on patent rights is set out in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patents (and other statutory intellectual property rights based on inventions)". CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The Workshop participants have made every effort to ensure the reliability and accuracy of the technical and non-technical content of CWA 17260, but this does not guarantee, either explicitly or implicitly, its correctness. Users of CWA 17260 should be aware that neither the Workshop participants, nor CEN and CENELEC can be held liable for damages or losses of any kind whatsoever which may arise from its application. Users of CWA 17260 do so on their own responsibility and at their own risk.

Introduction

Physical security equipment and systems are very diverse in technology, concept of operation, application area and performance, making security products difficult to compare in terms of performance, accuracy, usage, trust and validation of functionality. This guideline focuses on the functional performance aspects of certification for physical security products used for security of people, property and infrastructure, including:

— Barriers and building components (e.g. fences, gates, windows, doors, vehicle barriers, shutters);

— Access management (e.g. locks, safes, access control, biometrics);

— Surveillance (e.g. video surveillance systems, security lighting);

— Detection (e.g. intruder alarms, CBRN, explosives and weapons detectors).

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. A generic framework to accommodate these disparate types of scheme, whilst enabling harmonization is proposed by ensuring or encouraging:

— Performance measurement schemes which provide certified measurement of performance attributes, as well as threshold performance schemes which certify conformity with defined threshold performance values;

— Common definitions of performance attributes and their evaluation methods in measurement standards or test methods;

— Common threshold minimum performance values or grade definitions for conformity assessment;

— Common, or mutually accepted, processes for evaluation, certification and accreditation to ensure consistency over time and between participants;

— Common requirements and mutually accepted processes for ongoing surveillance to ensure the consistency of product manufacturing;

— Common or mutually accepted security marks.

Security products differ from other types of product in that they help protect against attacks by an intelligent adversary with malicious intent. Attackers are likely to:

— Constantly probe for and exploit weaknesses in the products;

— Attack in predictable and unpredictable ways;

— Constantly adapt and change their method of attack.

Consequently, schemes need to focus on realistic and adversarial testing; support evolving threats and requirements; and support mechanisms to handle security sensitive information.

The framework and guidelines are based on the ISO/IEC 17000 series of standards supplemented with features that focus on these security-specific aspects.

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 physical security products are unregulated in terms of their functional performance and the framework needs to support both voluntary and regulatory schemes.

The guidelines made in this document can be adopted in a way that fits best the requirements of the market.

This CEN Workshop is proposed based on the scope, objectives and the outcomes of the HECTOS project. HECTOS has received funding from the European Union Seventh Framework Programme FP7/2007-2013 under grant agreement no. 606861.

1 Scope

This CEN Workshop Agreement provides guidelines on how to design certification systems and schemes for physical security products and presents a framework in which these systems and schemes can be upheld. Physical security products include products which provide protection of people, property and infrastructure from acts of malicious intent, such as physical attacks.

It does not cover IT or cyber security and does not include products for safety, for instance protection from natural disasters. This CWA focuses on schemes for standalone security products and system components rather than systems and services based on these products and components.

Whilst there are several types of performance indicator for physical security products, this CWA focuses on their functional performance, not on aspects such as interoperability and environmental factors. Functional performance encompasses the security performance features of these products where sophisticated testing is often required. Schemes may also include other types of requirement such as interoperability, reliability, usability and resistance to unauthorised tampering.

The framework is based on the ISO/IEC 17000 standards series, supplemented with features that take account for the particular nature of security products:

— Realistic and adversarial testing;

— Continually evolving threat;

— Security sensitivity;

— Diverse range of products and applications.

The wide range of types of product and application, the need to operate in both regulated and unregulated environments as well as physical security products with very different maturity and market sizes, means that a range of different types of certification scheme are needed. Hence, the framework comprises a top-level structure with certification systems for performance measurement as well as systems for assessment of conformity with threshold performance requirements. .

This CWA targets stakeholders in the physical security product area such as user organisations and manufacturers; standards and certification bodies; governments and regulators who are involved in policy, setting up, operating and maintaining schemes.

Before new or additional standards and certification schemes are developed, a full impact assessment should be conducted to justify the need for standards and the potential costs incurred. Any certification schemes and standards for physical security products must:

— be operationally practical and proportionate to the threat that they seek to address, and be targeted to and tested in the real environment in which they are to be implemented in a manner relevant to the security threats in the applications where they will be implemented.

— not add unnecessary costs or delays for equipment manufacturers, or risk impairing Europe's capacity to swiftly develop, adapt or deploy equipment that can combat emerging security threats.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN ISO/IEC 17000:2004, *Conformity assessment — Vocabulary and general principles (ISO/IEC 17000:2004)*

EN ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025)*

ISO/IEC/TR 17026, *Conformity assessment — Example of a certification scheme for tangible products*

EN ISO/IEC 17067:2013, *Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes (ISO/IEC 17067:2013)*

ISO/IEC Guide 2:2004, *Standardization and related activities — General vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000:2004 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
certification
third-party attestation related to product attributes

[SOURCE: ISO/IEC 17000:2004, 5.5, modified]

3.2
certification scheme
certification system related to specific products, to which the same specified requirements, specific rules and procedures apply

[SOURCE: ISO/IEC 17067:2013, 3.2, modified]

3.3
certification system
rules, procedures and management for carrying out certification of measured product performance values or of conformity with defined threshold performance values

[SOURCE: ISO/IEC 17067:2013, 3.1, modified]

3.4
conformity assessment
demonstration that specified requirements relating to a product are fulfilled

[SOURCE: EN ISO/IEC 17000:2005, 2.1, modified]

3.5
evaluation body
organisation with technical competence, facilities and resources to carry out product testing according to the identified standards

3.6
functional performance
functional performance of a physical security product are the attributes of the product that relate to its function in mitigating an attack

3.7
inspection body
organisation which carries out inspections of a manufacture's production facility as part of the surveillance process to ensure continuing product quality and consistency of performance

3.8
measurement standard
standard specifying how attributes of an object shall be measured

3.9
performance measurement
determination of the value(s) of the performance attributes (testing) of a product

3.10
performance measurement scheme
certification scheme providing certification of the results of measurements of specified performance attributes

3.11
product standard
standard specifying requirements to be fulfilled by a product

[SOURCE: ISO/IEC Guide 2:2004, 5.4, modified]

3.12
scheme operator
organisation carrying out certification activities in a specific certification scheme

Note 1 to entry: Certification activities are included in the features of certification schemes.

3.13
system group coordinator
organisation or a group of organisations responsible for the basic rules, procedures, management, integrity and coordination among a group of certification systems

3.14
system owner
organisation or a group of organisations responsible for rules, procedures, management and integrity of a specific certification system as well as coordination of the different certification schemes it comprises

3.15
test method
specified method used to evaluate a product

3.16
third-party conformity assessment activity
conformity assessment activity that is performed by a person or body that is independent of the person or organisation that provides the object, and of user interests in that object

[SOURCE: ISO/IEC 17000:2004, 2.4]

3.17
threshold performance scheme
certification scheme providing certification that specified performance attributes conform with specified threshold performance values

4 Symbols and abbreviations

CBRN	Chemical, Biological, Radiological and Nuclear
QMS	Quality Management System
VSS	Video Surveillance System

5 Rationale for the framework

There is an important difference between physical security products and most other types of product. Security products help protect against threats from intelligent adversaries with malicious intent. These adversaries can be expected to:

— Constantly probe and exploit weaknesses of products;

— Attack in predictable and unpredictable ways;

— Constantly adapt and change their type of attack.

Physical security products cover a very wide range of product categories and applications. Products of a given type may also have a very wide range of performance requirements depending on the application.

Consequently, a number of special features need to be built into performance measurement and conformity assessment processes in security certification schemes, in order to take these aspects into account. These include features covering:

— **Realistic and adversarial testing.** The functional performance of security products is often defined in terms of the degree of protection they offer from real threats, for example how long a barrier resists a physical attack, or the percentage of threats detected by detection equipment. Users require realistic testing and, in some cases adversarial testing where the tester will probe and explore weaknesses of the product under test.

NOTE A realistic test uses real-world threats and scenarios. These may involve the use of humans e.g. to use a tool to attack a barrier or to conceal a threat on their body. Adversarial testing goes one stage further; here the attacker studies the product to determine its weaknesses and then designs and carries out the attack to exploit those specific weaknesses. In both cases, tests should be made as consistent and repeatable as possible, although this can never be done as precisely as for more artificial 'laboratory' tests which purposefully sacrifice realism for repeatability.

— **Consistency in testing.** In particular for tests involving human strength and skills, it is important to standardize testing so that testers do not apply too much or too little strength or skills. This contrasts with most proficiency testing where it suffices to have a tester with skills or measurement accuracy above a given threshold. Particular care needs to be taken in the design and implementation of inter-laboratory comparisons to ensure that different test laboratories are consistent, as well as to intra-laboratory comparisons to ensure that testing is consistent over time within a single laboratory.

— **Complex performance information.** Performance information such as detection rates is often complex and needs to be very precisely defined in standards and test methods. Sophisticated test procedures often need to be defined in order to ensure statistical accuracy.

— **Security sensitivity.** It is sometimes necessary to restrict access to product performance requirements, test methods and test results in order to prevent residual weaknesses and gaps from being identified and exploited by a malicious agent. Obscuring information on the performance of security products also helps increase the deterrent effect that their use can provide.

— **Requirements which continually evolve.** Changing threats lead to constant change in product requirements. Standards and test methods for security products need to be updated regularly to accommodate these changes. Where possible, there need to be mechanisms to minimize the amount of retesting that needs to be carried out and to ensure that the scope and validity of product certificates reflects changing standards.

— **The wide range of applications and performance requirements.** Many security products are used in a variety of different applications subject to different threats with a range of different performance requirements. The scope of performance measurement and threshold performance conformity assessment needs to be clearly stated to ensure that testing covers the range of requirements and that there is clarity over for which applications a product is and is not certified.

— **The diverse range of types of product, markets and levels of maturity.** Security products span a huge range from low cost consumer products selling in millions for a few Euros to specialist equipment costing millions of Euros and with only a handful of sales per year. Some products are very mature and stable; others are new and subject to rapid evolution.

The certification framework described in these guidelines accommodates these features.

Security products in several categories have anti-tamper features, especially those products used in electronic security systems involving a network of linked components, such as alarm systems, VSS, electronic access control and biometrics. Although they are not directly functional performance, these anti-tamper attributes share some of the special features of security products and have similar certification requirements.

6 Framework for harmonized certification of physical security products

6.1 Key features of the framework

The framework is a three-layered structure with an overall system group comprising a set of certification systems, each with a number of specific schemes. As in the ISO/IEC 17000 standards series, the term certification scheme denotes a set of rules and procedures for carrying out certification of a specified product type or application to which the same specified requirements apply; whilst a certification system is a set of certification schemes with some common rules and procedures, which will be managed at system level. Hence, systems will often group together schemes for related products since they apply common rules and procedures. The schemes will have a management function responsible for maintenance and operation of the scheme.

The framework accommodates all forms of conformity assessment including pass/fail testing against a threshold and performance measurement schemes. Typically, for a threshold performance scheme, product or application requirements will be set out in a product standard. For a performance measurement scheme, the evaluation process will be defined in a measurement standard (also known as test method). These scheme types are described further in section 6.3 below.

Figure 1 shows this three-layered structure. The system group level provides an overall common structure and a security mark - a security-specific quality mark indicating that a product has been certified according to the common framework.

Individual systems typically cover the certification of products in a particular group (and sometimes applications) such as building components, alarm systems, locks, and explosives detection equipment, each having their own specialist subject matter expertise and application requirements.

Schemes within each of these systems certify one or a group of closely related product or requirement types each with its own standards and/or test methods, setting out a specific set of requirements. These individual product certifications within a scheme are also defined by other controlling documents for ensuring consistency of conformity assessment activities (see section 6.6).

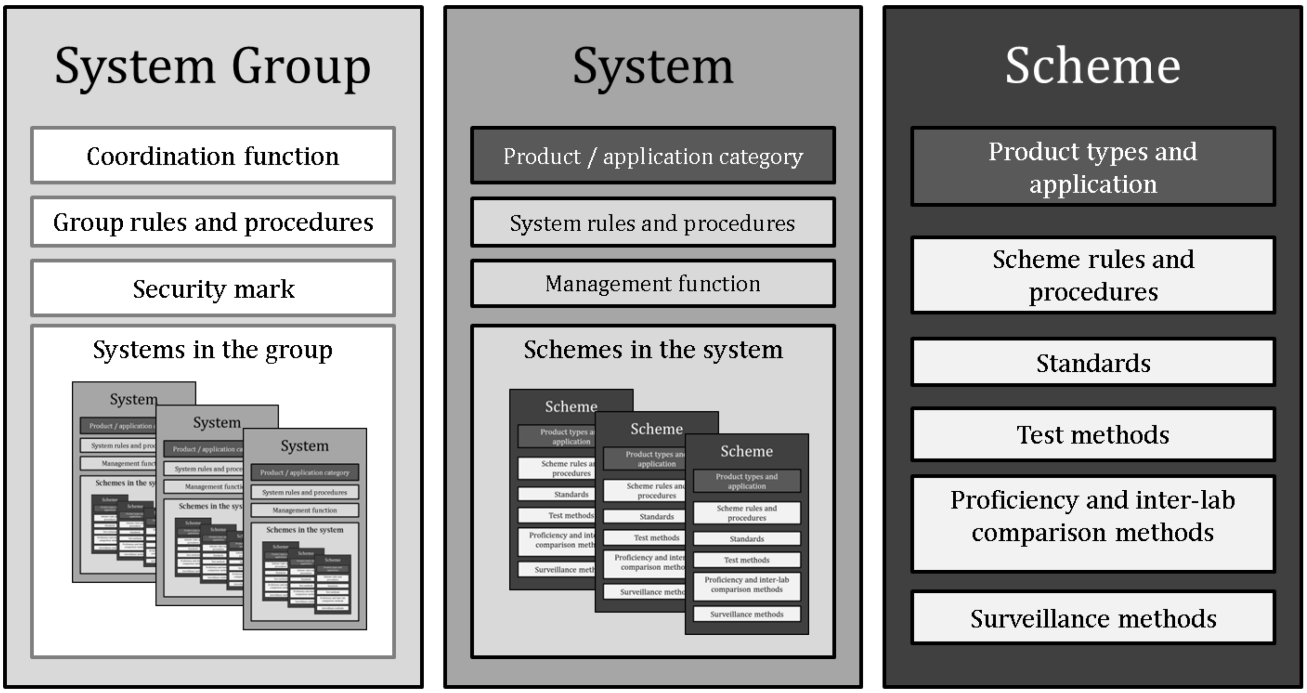

Figure 1 — Certification systems and schemes – key building blocks

Note that the system structure is only required when there is more than one scheme with common rules and procedures. In the case of a single scheme, the system and scheme roles are combined.

6.2 Certification framework organisational structure

Figure 2 shows the three layers of the certification framework for harmonized schemes, illustrating how certification systems and schemes can accommodate different product types and applications, and how they relate to each other.

The overall security mark and management procedures that apply to all the constituent systems and schemes are defined at the top system group level.

The system level includes management procedures and special rules that apply to particular product groups.

Scheme specific structures and controlling documents are defined at the scheme level. Of particular importance are: scheme rules and procedures, standards and test methods, and inter-laboratory comparison methods that ensure that all operators in the scheme test and certify in a consistent manner.

System committees and **working groups**, with expertise in the product category and its application areas, are important in the certification operational structure. They ensure that the technical knowledge required to evaluate products in a consistent way is shared between participants and that working practices can be refined and improved in the light of experience, as well as providing a link to standards organisations. The system committee spans different schemes within a system, and the working groups bring together the different participants within a single scheme. System committees and working groups can have a similar structure to those of European and international standardization organisations (although there will not necessarily be a 1:1 correspondence between the two).

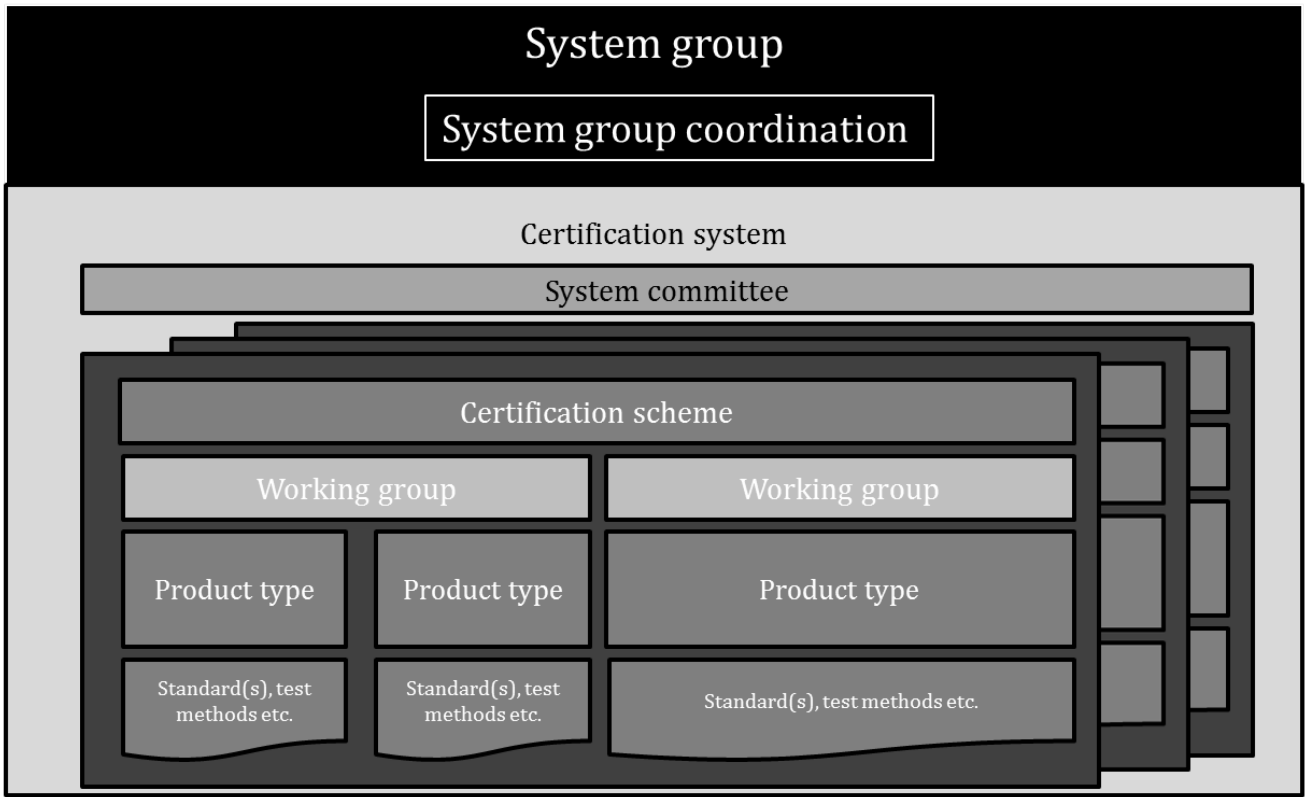

Figure 2 —Framework for harmonized certification systems and schemes of physical security products

System committees and working groups should work closely with each other and with the technical committees and working groups of the standards organisations to help manage and expedite changes to both standards and certification schemes in response to changing threats and ensure that the standards and other controlling documents which underpin a scheme remain fit-for-purpose. To further ensure acceptance of standards and schemes, it is important that all stakeholders, especially end user organisations are included in this process to the highest extent possible.

This structure ensures that systems and schemes for all the wide range of different security product categories and applications can be included within the framework under a common overall management and a common security mark, and that an appropriate level of technical expertise and focus can be applied to ensure its proper functioning. The aim of the structure is to minimize unnecessary complexity and duplication by enabling rules and procedures that apply to several categories to be defined and maintained once at group or system level and then to be 'inherited' by schemes and product certifications at the lower level. The structure also enables consistency to be maintained between the different certification bodies that participate in the schemes.

Whilst the three-layer structure is designed to accommodate all the different types of security product and application, the full structure may not be needed for every product category. The needs of the market will ultimately determine the extent to which the structure is implemented since market acceptance will depend on the value created by the certification services relative to their cost, as well as the ability by market stakeholders to participate in and shape those services to their needs.

6.3 Scheme types

The functional performance of a security product, such as the resistance of a barrier, the recognition capability of a biometric product or the threat detection performance of an explosives detector, can depend on many variables and be complex to define and measure. Performance values obtained can vary significantly, depending on the way performance is defined and on the way it is measured. In addition, the wide variety of different application requirements and the fact that products are often used in combination with others to achieve a security objective means that there is often no commonly agreed threshold performance value that can be used to define an 'acceptable' product.

Accordingly, there is a need for schemes that provide trusted measurements of the values performance attributes, as well as the more well-known types of scheme which assess conformity with a defined threshold performance value.

The framework and approach described in these guidelines supports both types of scheme:

— **Performance measurement schemes** – describe the way that product performance attributes are defined and describe in detail how they are measured. They are based on measurement standards and produce a statement of test results which can be independently certified;

— **Threshold performance schemes** – define requirements on product performance attributes (in the form of threshold performance values or performance grades) and describe in detail how conformity is determined. They are based on product standards and produce a statement of conformity with the specified requirements, which can be independently certified in terms of both the results obtained and the process used to measure the performance.

The type 1 to 5 schemes, as defined in ISO/IEC 17067, are all applicable to both performance measurement and threshold performance schemes.

The choice of scheme type is made based on criteria including the:

— Range of performance requirements in different applications;

— Market size and maturity for a particular application;

— Regulatory requirements of specific products and applications;

— Complexity, number and dimensionality of the relevant performance attributes (for example receiver operating characteristic (RoC) curves of detection systems) and

— Ways that products are deployed in combinations in layered security systems such that performance gaps in one layer can be compensated by capabilities in another.

Threshold performance schemes can use different performance grades when appropriate, e.g. to cover a wide range of performance requirements originating from different applications or local variations.

Importantly for encouraging innovation and the introduction of new security capabilities, performance measurement schemes provide trust whilst not preventing products, which provide some useful capability but cannot meet all the performance requirements in a standard, from entering the market.

Finally, note that schemes may be hybrid schemes where some attributes have threshold performance requirements and others where the requirement is just for measurement of the attribute according to a measurement standard.

Even though the framework focuses on certification (third-party attestation), self-testing is still applicable using common test methods defined in measurement standards. This can provide valuable information for stakeholders in emerging and fast changing markets.

6.4 Common database and security mark

The external 'brand' of the overall framework can be asserted by a security specific quality mark, which is to be applied to all certified products. This may incorporate specific system/scheme marks and identifiers, and the standards/test methods associated with it. Where applicable, it can also include the performance grade met by the product. Product certificates follow a similar marking/numbering hierarchy.

A centralized online database with information about the product and its certification should be provided by the system group coordinator. The mark should provide easy access to the database.

NOTE Certification bodies may add their own marking in addition to the overall security mark.

6.5 Management and operation

6.5.1 General

This section describes the roles of the various actors in the framework: system group coordinator; system and scheme owners; together with the scheme operators who are the participants in the scheme. Schemes are operated by one or parallel scheme operators: certification bodies. The certification bodies typically appoint one or a number of evaluation bodies to carry out evaluation activities. Inspection bodies may also be appointed for production inspection activities. Operators may participate in the certification or evaluation of some or all product types/standards within a scheme.

An overview of system and scheme actors within the framework is given in Figure 3.

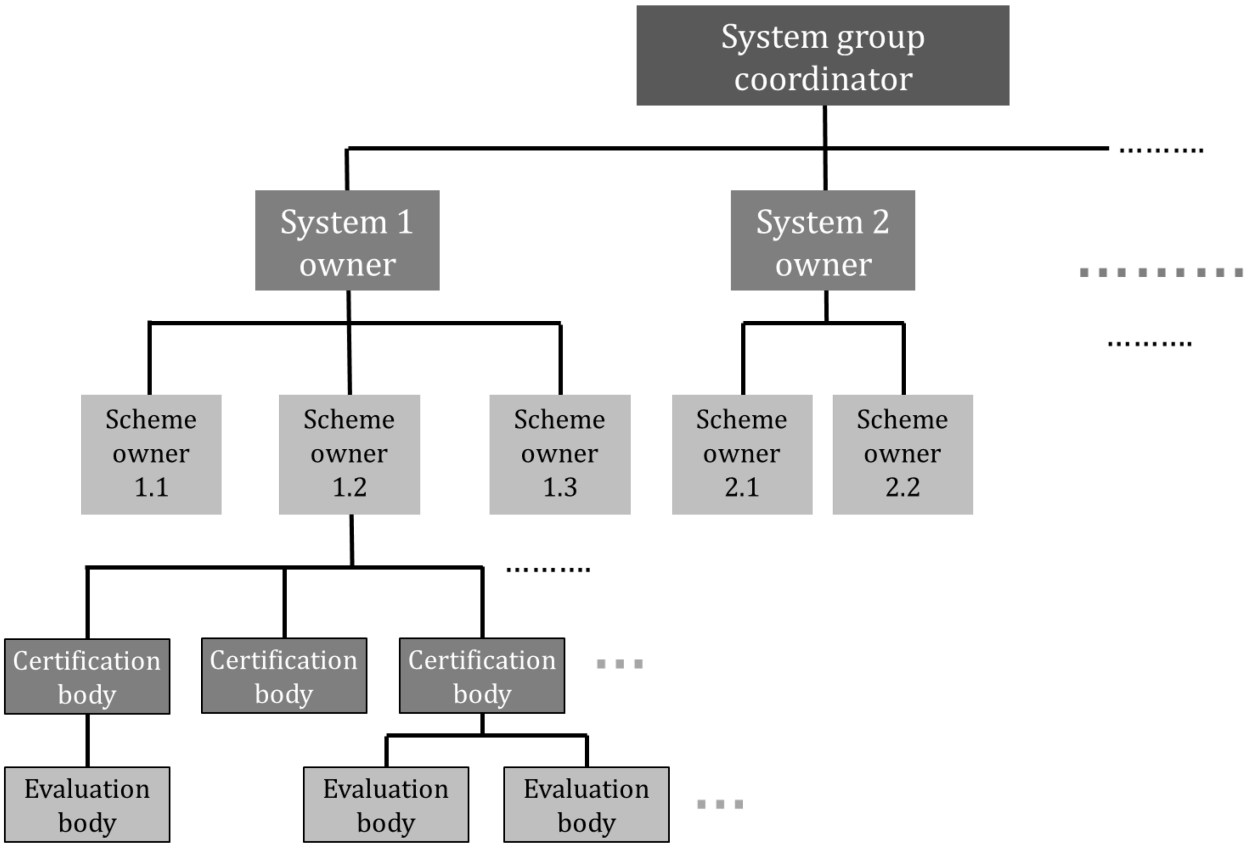

Figure 3 — Actors within the framework for harmonized certification

A summary of the system and scheme actors and their roles is given below. Depending on the particular scheme, market size and maturity, some roles may be merged. A single organization may also take ownership of several roles within the structure.

6.5.2 System group coordinator

The system group coordinator is responsible for defining, monitoring and enforcing the underlying rules, procedures, management, and coordination among the different certification systems it bridges, including upholding the rules and requirements of the security mark. The system group coordinator shall be an independent organization such as the European Commission, another governmental body or a balanced consortium of stakeholders comprising users, certification bodies, regulators and producers/distributors.

Roles: Coordination between systems; management of mark usage; management of framework; manages database.

6.5.3 System owner

The system owner is authorized and regulated by the system group coordinator and is responsible for rules, procedures, management and integrity of the system and the different certification schemes within it.

The system owner could be one or a group of national governmental authorities, regulatory authorities, certification bodies, an industry group or trade association, or other organisations independent of the production or sale of the items certified in the system.

Roles: Define system scope – applications/product categories; development of system rules and procedures; management of system and scheme owners; lead system committee; support system group management.

6.5.4 Scheme owner

The scheme owner is an organization responsible for developing and maintaining a specific certification scheme. The scheme owner coordinates the associated scheme operator(s) via the working group. The scheme owner could be a governmental authority, a regulatory authority, an industry group, a trade association, a group of certification bodies or other organization independent of the production or sale of the items certified in the scheme. The scheme owner is responsible for the rules, procedures, and integrity of scheme operators.

The scheme owner can be the same organization as the system owner.

Roles: Development of scheme rules; procedures; manage scheme operators; working with standardization organisations on maintenance of standards and test methods; inter-laboratory comparison methods; surveillance methods; lead technical working groups; support system group management.

6.5.5 Scheme operator

A scheme operator is a certification body responsible for operating parts of a specific certification scheme under a particular system. A single scheme can have multiple operators running parallel instances of that scheme, all acting under the coordination of a scheme owner. Several scheme operators may exist in one country. A certification body may be an operator for all or several parts of schemes in one system or for schemes across different systems (see Figure 4).

Roles: Conduct conformity assessment activities; issue product certificates and marking; selection and coordination of evaluation bodies and inspection bodies; participation in working groups and committees.

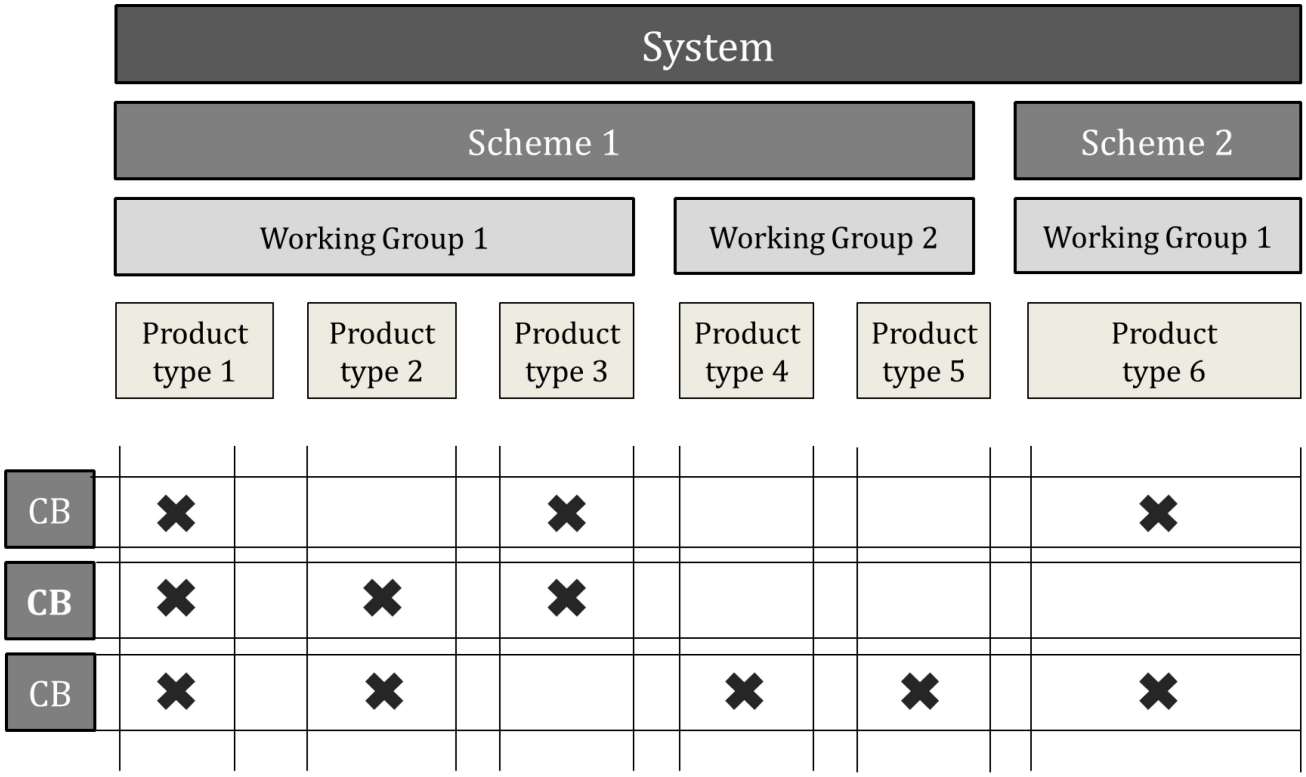

Figure 4 — Example mapping of certification bodies onto schemes showing how a certification body (and its associated evaluation and inspection bodies) may be an operator for a number of different products, schemes and systems

6.5.6 Evaluation body

An evaluation body is a test laboratory that has the technical competence, facilities and resources to carry out the product testing according to the identified standards and has accreditation according to the relevant product standard. The scheme operator may carry out the evaluation function itself or may appoint one or several evaluation bodies. A scheme operator may apply specific selection criteria (for instance additional criteria on top of the general requirements in ISO/IEC 17025) in the appointment of evaluation bodies and inspection bodies. Allocation to an evaluation body is carried out by the scheme.

Roles**:** Execution of testing; participation in working groups; inter-laboratory comparisons.

6.5.7 Inspection body

An inspection body carries out inspections of a manufacture's production facility as part of the surveillance process to ensure continuing product quality and consistency of performance. The inspection body may be part of the certification body or may be a separate organization.

Roles: Execution of production facility inspections; participation in technical working groups.

6.6 Controlling documents

At the system group level, a framework set of documents will exist, describing overall basic rules for participation and the terms for usage of a common security mark. The system level will further develop a set of key documents describing common rules and procedures for all constituent schemes.

The approach taken in establishing separate schemes will depend largely upon the identification and review of existing standards around which a scheme can be formed. A scheme, as described in section 6.1, is defined in terms of its rules and procedures, some of which are passed down from the system and system group level, and a set of product certification specific technical controlling documents specific to each product certification.

6.6.1 Scheme Controlling Documents

The scheme will have operational documents defining processes for certification and certification maintenance of all of the products in the scheme. These are described in the next two sections of this document. A scheme will also have controlling documents for the participation to the scheme. For example the certification bodies, test laboratories, inspection bodies and so on will need to be qualified according to scheme requirements in order to participate in the scheme. Those requirements and the procedures to apply them will be defined in scheme controlling documents. Other scheme controlling documents may define the methods and procedures for ensuring consistent results from all scheme participants and may include peer assessment and/or proficiency testing, etc.

6.6.2 Product Certification Controlling Documents

Each product certification within a scheme is defined by a set of controlling documents which set out the specific technical product and evaluation requirements as well as the product-specific technical aspects of operational processes and procedures such as proficiency testing and surveillance.

For threshold performance schemes, these will include, at top level, a **product standard**, which sets out the functional performance (and other) requirements, typically as a threshold performance, together with a scope defining the product types and applications to which the certification applies.

Threshold performance schemes will also be supported by one or more test methods, either as part of the product standard or a separate measurement standard.

For performance measurement schemes, the top-level document will be a **measurement standard** (test method), setting out testing requirements, which need to be sufficiently detailed to remove ambiguities which might cause inconsistency in application.

Hybrid schemes will have standards with both types of requirement.

Both types of scheme need a **proficiency testing document** defining how proficiency testing should be carried out, using intra and inter-laboratory comparisons, peer assessment and other techniques to ensure that the specific product testing or other aspects of the scheme are applied consistently over time and across different participants in the scheme.

The **certificate specification** defines the technical information about product performance that is included in the product certificate.

Finally, for schemes which include periodic surveillance (e.g. type 5 scheme in ISO/IEC 17067:2013) of ongoing product production, a **surveillance method** is required to define the technical aspects of this product surveillance, again to ensure quality and consistency between participants.

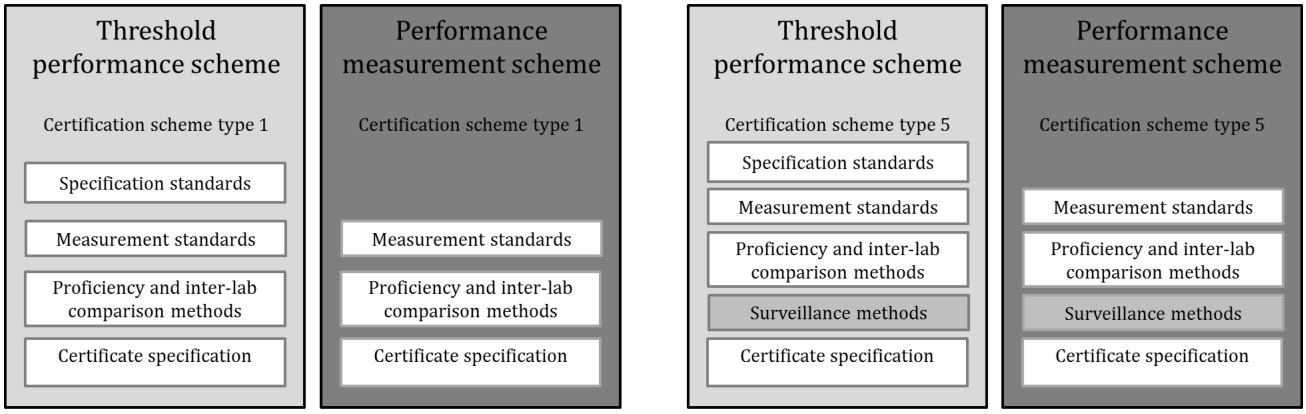

Figure 5 — Product certification controlling documents for threshold performance and performance measurement schemes

These documents play a key role in ensuring the quality and consistency of schemes, which is of particular importance given the complexity of security product performance definition and measurement. The documents are valuable in supporting the qualification and accreditation process of scheme operators and participants (certification bodies, evaluation bodies, inspection bodies), in order to ensure consistency across operators, both within and between different countries.

7 Guideline for establishing a certification scheme

The framework accommodates a wide variety of schemes, defined by product types and their standards. Where appropriate, and where both value creation and market acceptance can be demonstrated, a scheme can also be defined by a specific application of a group of products, e.g. explosives and weapons detection in aviation security. For these, it is important to consider the application users, threats and environments for the envisaged product types. In this section, a product type 'bottom-up' approach is taken as the starting point for establishing a scheme. To accomplish this, a template is introduced to systematically address the actions for establishing a certification scheme. The template is designed for adding a new product certification to a scheme or adding a new scheme to an existing system. Whilst the template with its bottom-up approach provides useful guidance, a top-down approach is also required in order to ensure that the broader system- and group-level issues are considered.

The template for establishing a scheme provides the steps to take, and scheme features and functions to consider, in order to establish a certification scheme for physical security products under the certification framework. The template is generic and designed to meet the needs of a wide range of schemes addressing diverse product types and applications.

Nine groups of activities and questions are described. These should be actioned and answered by those leading the establishment of the scheme – the prospective scheme owner supported by a preliminary scheme working group. Typically, this working group, comprising stakeholders and technical experts, will be involved in such a way that the template sections can be addressed in parallel and re-visited in an iterative process.

The particular order of activities is not necessarily fixed, and will depend upon the existing maturity of elements defining the scope of the scheme (e.g. standards, products and test methods) and the driving forces and priorities of those establishing the scheme. The template serves to guide the sequence of activities needed and as a checklist to ensure all relevant scheme requirements have been included. The template addresses steps in the establishment of security product schemes and systems in order to facilitate consistent implementation. It is designed as a "pick and choose" guideline – i.e. schemes that do not benefit from all of these steps do not need to apply them.

The template as presented here assumes that the starting point for establishing a new scheme is at the level of the product type(s) around which the certification scheme should be designed and built. Scheme development will further identify existing systems to which the scheme could belong. When a scheme is added to an existing system, rules, procedures and structures are already in place and supported from the system group coordinator and can be handed down and adopted. An iterative push-pull of requirements and features between scheme and system will help define the optimum arrangement and structure.

In deciding whether different product types should be grouped into the same scheme, the following attributes and characteristics should be considered to identify similarities or key differences:

— Scheme type: performance measurement or threshold performance;

— Functional requirements;

— Applications of use and operational environment;

— Test methods and materials;

— Links to standardization technical committees and working groups;

— Stakeholders expected to be involved in operation of the scheme;

— Surveillance methods;

— Dissemination level and regulatory considerations;

— Market size and maturity;

— Certification rules and procedures and

— Security sensitivity.

In a top-down approach, established systems can also seek to identify existing or emerging product types and applications which could be adopted into an existing scheme or developed as a new scheme on the basis of demand and ownership from proposed scheme level actors.

Figure 6 presents the process chart for establishing a scheme and system. The detailed process descriptions are given in the remainder of this section.

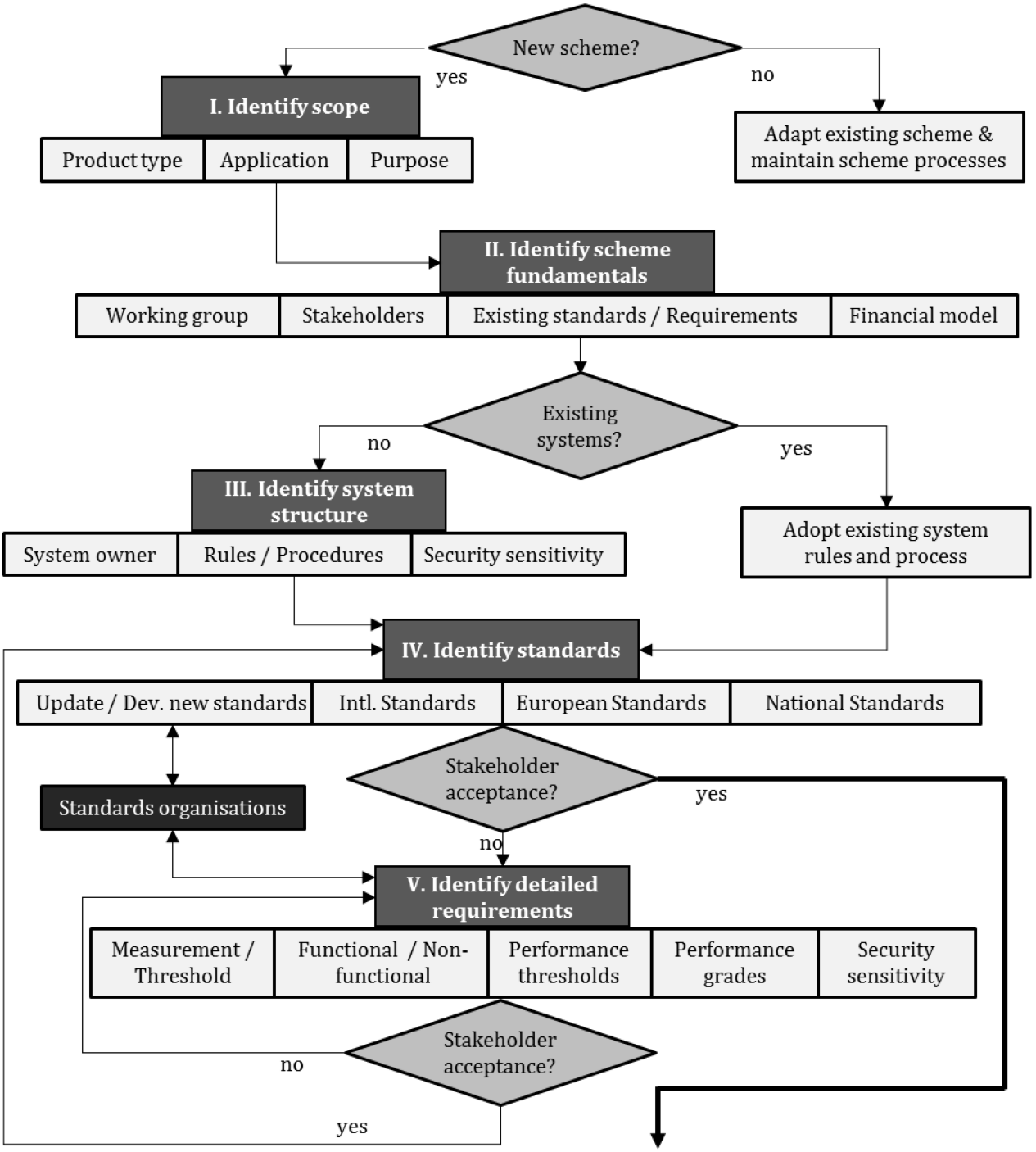

Figure 6 (1 of 2) Template for establishing a certification scheme and system. Stakeholders comprise end-users, suppliers, manufacturers, certification bodies, evaluation bodies and, when applicable, regulators

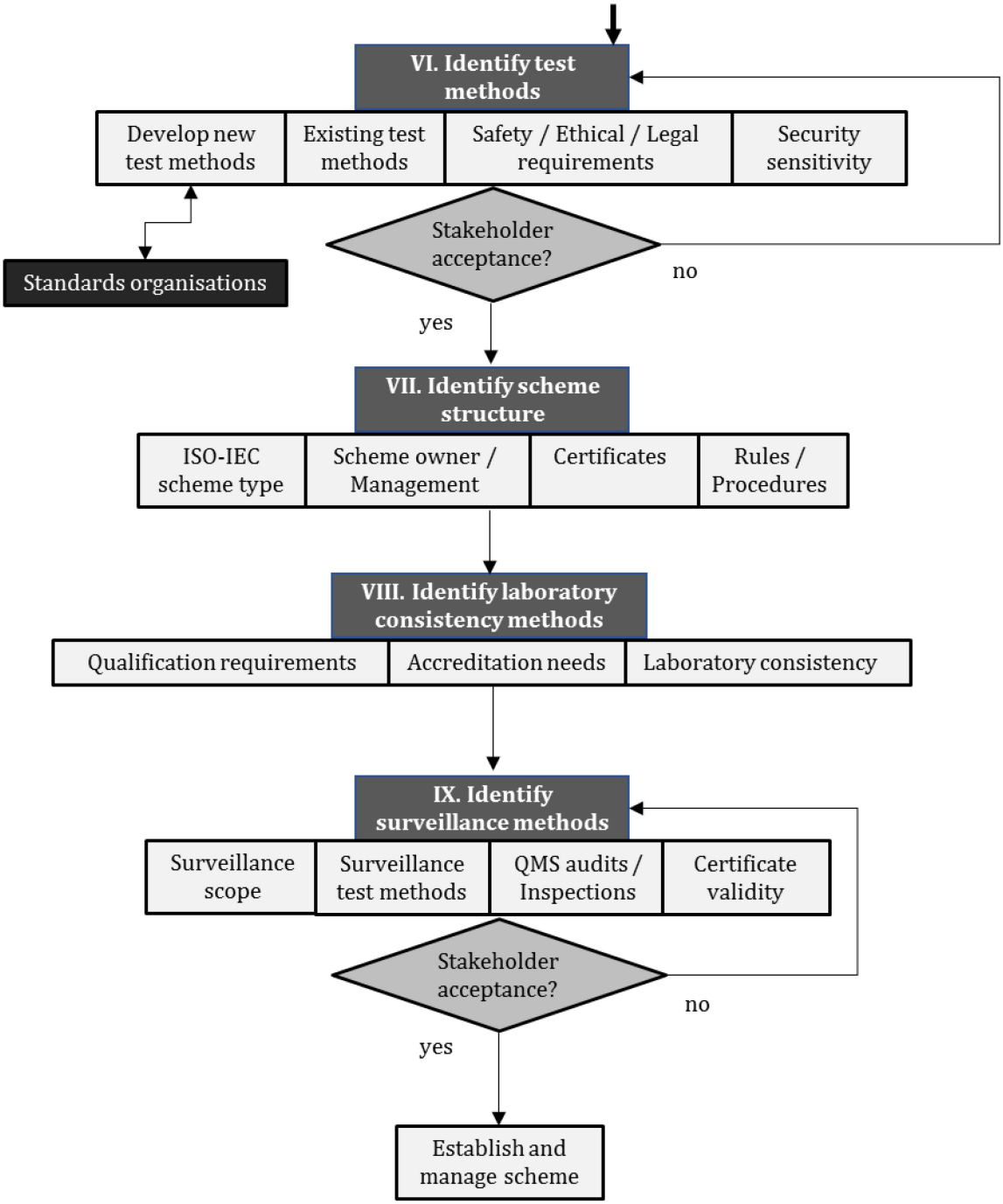

Figure 6 (2 of 2) —Template for establishing a certification scheme and system. Stakeholders comprise end-users, suppliers, manufacturers, certification bodies, evaluation bodies and, when applicable, regulators

I) Identify the ***scope of the scheme***, it is based upon:

I.1 Product type(s): Identify physical security products types for the scheme e.g. mechanical locks, alarms, biometric access control, explosives detection. Consider the range of product types and the technologies used.

I.2 Application: Identify end-user applications e.g. train station security, open public spaces. Consider application end-users, security threats and the environment for the envisaged product type use.

I.3 Identify purpose of scheme: Providing information and assurance to end-users, meeting high-level needs such as providing protection for the public, support fair competition growth via a free and single market for industry. Consider the purpose(s) of the scheme such as: demonstrating compliance with regulations, demonstrating compliance with existing standards, providing trusted product performance data for designers, providing a quality mark to assist for non-expert purchasers, etc.

II) Identify ***scheme fundamentals***

II.1 Establish the prospective scheme owner and a preliminary working group: A scheme overarching working group should be convened early on and will be responsible for establishing the scheme. This working group should lead scheme establishment activities and make decisions based upon this template.

Typical members in the preliminary working group are the organisations that would participate in or benefit from the scheme, such as end-users and technical experts from evaluation and certification bodies. Other members could be government application experts and policing or security services. Manufacturers are also beneficiaries and can be involved in the establishment of the scheme.

II.2 Identify stakeholder groups: Establish motivation, acceptance and demand across relevant groups of users of the proposed scheme. The survey should include scheme operators, manufacturers, end-users, governments, the public and regulators.

II.3 Perform an initial survey of existing standards and requirements landscape: Scan existing standards related to the proposed scheme scope and its product types. Identify sources of requirements, e.g. binding or non-binding, - users or regulators; this will influence the nature of the scheme – voluntary or mandatory - and the authority/mandate of the system. A wide survey will ensure that all relevant standards and requirements are considered before initiating a detailed assessment of relevant standards.

II.4 Identify a financial model: Develop a business model for owning and operating a certification scheme. Identify likely costs for product manufacturers and suppliers. Identify how the costs and financial rewards for managing and operating the scheme should be distributed amongst participants.

III) Identify ***system structure***

III.1 Identify existing systems: Identify whether an existing certification system could accommodate the proposed scheme or product type. If such a system exists, assess if it needs to be modified or extended or if it is immediately applicable.

III.2 Identify system owner and management: Where there is no existing system, identify who should be the system owner. Identify system management functions, rules and procedures. Initiate dialogue with system group coordinator about setting up a new system. Consider what system level management functions, rules and procedures would be needed to support the proposed scheme and which other schemes should be covered by the system.

III.3 Identify security specific management: Identify rules and procedures for handling security sensitivity (if needed).

IV) Identify ***standards***

IV.1 Identify relevant product and measurement standards: Identify relevant international and European standards that define functional and non-functional security product and application requirements. Identify relevant standardization organisations' technical committees and working groups or industry associations that have specified security product requirements.

IV.2 Identify harmonized and local standards: Identify additional national standards that may be bolted onto a harmonized base-line standard.

IV.3 Identify need to develop new standards: In some cases there are no immediately applicable product standards to be found, e.g. they might not address all requirements, they might be local standards with diverse requirements, or the required test methods might not be specified.

IV.4 Review stakeholders acceptance of identified standards: Identified existing standards and any need for any harmonization and development should be accepted by stakeholders. Explore the stakeholder's motivations for the development of new or updated standards.

V) Identify ***detailed requirements***

V.1 Establish performance measurement and threshold performance scope: Determine whether the certification scheme will be a performance measurement or a threshold performance scheme.

V.2 Identify functional and non-functional requirements: Identify the product functional and non-functional performance attributes and requirements. Identify non-functional requirements which are also addressed by the certification scheme.

V.3 Identify threshold performance and performance measurement requirements - Identify performance and threshold metrics e.g. delay time, detection true-positive- and false-positive rates.

V.4 Identify different and conflicting requirements: Identify differences in requirements based on geography, interoperability with existing local systems, historical differences, application differences etc.

V.5 Identify steps for achieving common view in case of conflicting requirements: Assess the possibility of accommodating geographic, application or user differences in a single scheme through use of performance grades, identified variations etc. Explore whether conflicting requirements can be harmonized by negotiation. Note that the scope of certification needs to be clearly stated and understood when application and user differences exist.

V.6 Identify the security sensitivity of information: Identify whether any of the information in requirements that may appear in product standards or measurement standards requires security classification according to national or European procedures. Schemes may also need procedures to handle material which is test-sensitive, commercially sensitive etc.

V.7 Review acceptance of requirements: Review requirements with scheme stakeholders, including manufacturers and end-user organisations. Stakeholder acceptance of the product and certification requirements is a prerequisite for a successful scheme. Reviews should be carried out with stakeholders at each step in the scheme design and action taken to resolve any issues. This is an iterative process and should occur throughout the process of establishing a scheme.

VI) Identify ***test methods***

VI.1 Survey and identify existing test methods: Determine whether test methods are detailed in existing standards. Survey whether any local test methods are also in use. Identify evaluation methods and reporting of complex performance metrics – e.g. based on threat types/scenarios, sensitivity settings, concepts of operation and application.

VI.2 Adopt existing test methods: Assess the suitability of identified test methods.

VI.3 Develop new test methods: Identify the need for development of new test methods for new or diverse technologies within the same product type or application. This includes development of realistic and adversarial type-testing, sampling, re-testing and self-testing methods. The test method(s) should be comprehensive, unambiguous and provide a sufficient level of granularity and statistical confidence (number of test runs). Repeatability should be supported, for example through

— *Consistent sample preparation* using the same methods and the same materials acquired from the same source (tangible examples include sample preparation for explosive trace detection, and artificial fingerprints for biometric presentation attack);

— *Environmental parameters* during testing need to be controlled and consistent (temperature, humidity, lighting, cleanness etc.). The equipment should be tested in realistic environments (where the equipment is likely to be used);

— *Minimizing demographic differences* between evaluation bodies in tests involving human test subjects (applicable for example to security scanner test persons, finger-prints);

— Including measures to support proficiency testing.

VI.4 Identify the security sensitivity level for test methods: Assess whether parts of the test method, for example threat items/substances or biometric presentation attack artefacts, should be detailed in classified annexes. A high-level unclassified description of the test method could be provided in order to facilitate distribution (also to manufacturers) and recognition of test method. Assess if there is a need to classify test results and in such case which levels of reporting is required.

VI.5 Identify ethical and legal compliance requirements: Establish whether the test method will include activities or aspects that fall under European and/or national regulations related to privacy or data protection. Identify any needs to perform/obtain privacy impact assessment, data management plans, ethical committee approval, consent forms for testing procedures, permits and safety requirements including for example risk assessments for handling of hazardous materials.

VI.6 Review acceptance of test methods: Review the stakeholders' acceptance of test methods, including the acceptance of test method adaptions and development.

VII) Identify ***scheme structure***

VII.1 Select ISO/IEC 17067 scheme types 1-5: Type 5 schemes are recommended unless there are specific reasons for not doing so. Choice determined by market, technology maturity, threat evolution and cost aspects such as test method complexity, re-testing cost and periodicity of surveillance activities etc.

VII.2 Identify scheme owner and management: The scheme owner is the organization responsible for developing and maintaining a specific certification scheme. Examples could be a governmental or regulatory authority, an industry group, a trade association, a group of certification bodies etc. Each scheme will be supported by one or more working groups depending upon the range of product types covered.

VII.3 Scheme certificate: Identify the information that should be included on the scheme certificate. Annex C in ISO/IEC TR 17026 is the baseline.

Detail the scheme-specific information that should be included alongside the security mark. Such information could include standard and performance grade.

VII.4 Identify scheme rules and classification: Identify scheme participant rules and procedures for working groups and scheme operators. Specific product type rules and procedures may also be required and should be managed by a nominated working group. Identify procedures for handling of scheme specific security sensitive information (if needed).

VIII) Identify and establish ***qualification methods*:**

VIII.1 Identify operator qualification requirements: Define general requirements for scheme operators to be qualified for participating in the scheme. For instance, the operators must be capable of doing the required work and agree to follow the scheme rules and procedures. They must be competent, have the necessary equipment for testing and inspection, and they must have trained and qualified people. They will also need to have appropriate QMS in place. All of this is usually covered under accreditation.

VIII.2 Identify accreditation needs: Identify common accreditation requirements and accreditation actors. Identify whether both scheme and system specific requirements are included. Assess whether any scheme and system add-on requirements are needed. For example, there may exist scheme specific accreditation requirements for operators handling hazardous substances or classified information. Identify the scheme actors that should meet accreditation requirements, such as certification bodies, evaluation bodies and inspection bodies.

VIII.3 Identify and establish laboratory consistency methods:

a) Methods should support consistency in performance and processes and inter/intra-lab proficiency testing especially for realistic and adversarial type testing. Examples of methods may be:

— Moderation of results (compare results within and in-between laboratories over time);

— Round robin tests;

— Common training course for testers.

Identify what test items are necessary for the inter- and intra-laboratory comparisons: for example single source test sets and test pieces.

b) Consistency is also supported by scheme-specific peer assessment procedures where operators periodically audit each other in order to monitor and benefit from for example

— application of scheme roles and procedures;

— testers' capability to interpret test protocols;

— testers' experience and skills.

The peer assessment programme should identify the periodicity of the audits.

IX) Identify periodic surveillance methods for ***maintenance of certification:***

IX.1 Determine surveillance needs: For instance, for the product(s) within the scheme, determine if the market requires that the manufacturer's production facility and processes should be audited, assessed and certified.

If surveillance is necessary, it can exist as one or more of the following:

a) Periodic testing/inspection of samples from the market (i.e. point of sale of the product);

b) Periodic testing/inspection of samples from production;

c) Periodic assessment of the manufacturers production facility and processes;

d) Periodic assessment of QMS of manufacturer;

For example, a scheme type 5 consists of a and/or b and c and/or d.

IX.2 Identify scope of surveillance test methods: Identify any need and form for specific surveillance test methods. Surveillance test methods can comprise sampling, full type tests or reduced tests, self-testing etc.

IX.3 Identify procedures and frequency of surveillance activities: Identify procedures for surveillance and define any inspection and testing in a surveillance method. Define methods to ensure surveillance activities are consistent.

IX.4 Identify validity of certificate: Consider scheme specific factors that could influence certificate rules and certificate validity period, for example likely frequency of updates to standards.

Bibliography

[1] EN ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles (ISO/IEC 17000)*

[2] EN ISO/IEC 17011, *Conformity assessment — General requirements for accreditation bodies accrediting conformity assessment bodies (ISO/IEC 17011)*

[3] EN ISO/IEC 17020, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection (ISO/IEC 17020)*

[4] EN ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025)*

[5] ISO/IEC/TR 17026, *Conformity assessment — Example of a certification scheme for tangible products*

[6] EN ISO/IEC 17030:2009, *Conformity assessment - General requirements for third-party marks of conformity (ISO/IEC 17030)*

[7] ISO/IEC 17043, *Conformity assessment — General requirements for proficiency testing*

[8] EN ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services (ISO/IEC 17065)*

[9] EN ISO/IEC 17067, *Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes (ISO/IEC 17067)*

[10] ISO/TR 19948, *Earth-moving machinery — Conformity assessment and certification process*

[11] The 'Blue Guide' on the implementation of EU products rules (2016)

[12] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*

[13] ISO/IEC Guide 98-3, *Uncertainty of measurement — Part 3: Guide to the expression of uncertainty in measurement*