European Cyber Security Certification

A Meta-Scheme Approach v1.0

WG1 – Standardisation, certification, labelling and supply chain management

DECEMBER 2017

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg1_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The current version of this document is focusing on the common denominator across products, services, systems, etc. For instance, the proposed levelling structure is very general and requires separate tailored considerations for products, services, systems, etc. which will be subject to refinements in the next evolution of this document. For instance, for large systems the emphasis might be more on process or company certification, whereas for components and devices the focus might be more on product certification. Section 2.3 is borrowing some terminology from the Common Criteria. Notice, this is **ONLY** the terminology and does not mean that Common Criteria itself is proposed here for the meta-level of the scheme.

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources including external websites referenced in this publication.

Copyright Notice

EXECUTIVE SUMMARY

A very broad set of security certification schemes exist for products, systems, solutions, services and organizations, but there is no unified or combined solution available, which makes it difficult to understand what is finally required to make things consistently secure.

In this document, ECSO introduces the concept of a meta-scheme. This meta-scheme will encompass many of the existing certification schemes (e.g. component certification, process certification, service certification, etc.). It will do so by evaluating the level of confidence in the security strength of a product, system, solution, service or organisation that results from a scheme used, and map this onto a harmonized set of levels defined by ECSO. These levels represent the level of confidence and the scope of security functionality of the item certified. The latter allows to clearly specify the security required. Each level is mapped to a single symbol that can be used for a label.

With the meta-scheme, it is possible to combine the advantages of different schemes, including integration steps on top. The integration steps allow some flexibility to overcome potential contradictions between schemes. Currently, this is not possible with one single existing scheme, as each scheme has dedicated focus on specific aspects of the market it is focused on; there is no “silver bullet” solution. In addition to the combination of existing and future schemes, the meta-scheme also allows the identification of “alternatives” (i.e., one can define that one out of many certification schemes is sufficient to pass a certification which gives more flexibility and saves costs). This allows for defragmented markets regarding certification variety across countries.

Moreover, the advantage of a meta-scheme approach is that it allows the addition of new schemes in the future, as it is not limited to any kind of existing subsequent scheme or the market considered.

TABLE OF CONTENTS

1 INTRODUCTION

Security and Privacy will continue to be a major concern for citizens and organizations, as well as important factors for the growth of the European economy. The connected society in Europe increasingly relies upon digital identities, digital processing of personal identifiable information, as well as digital control of physical world processes. Thus, trusting the security claims of products, systems, solutions, services and organizations[1] across the supply chain is essential. The recent WANNACRY attack showed that zero-days attacks[2] in widely-used platforms can break the security of products, and that mitigating risk and impact of known vulnerabilities is essential, like for example through applying existing patches or proper counter-measures.

The need for Security and Privacy is no longer limited to specific payment or governmental applications. With the deployment of the digital world and its ubiquitous connectivity, Security and Privacy is now a concern for every business and every citizen.

Industry organizations or citizens with no specific knowledge need to be able to quickly assess if an item will provide confidence that required Security and Privacy is provided. For example, a minimal required barrier may need to be set to deter, detect and respond to distribution and use of insecure interconnected items throughout Europe and beyond (IoT).

Security certification as a means of security assurance demonstrates conformance to a security claim for an item. Many certification schemes exist, each having a different focus (product, systems, solutions, services, organizations …) and many assessment methodologies also exist (check-list, asset-based vulnerability assessment …). Due to the complexity of the subject, the European Cyber Security Organisation (ECSO) Working Group 1 (WG1) "Certification, Standardization, Labelling & Supply Chain Management", launched in October 2016, has created two documents in the initial phase of the work:

- **Challenges of the Industry** (COTI) [1]
- **State-of-the-Art Syllabus** (SOTA) [2]

On the one hand, the COTI document is describing some of the challenges the industry is facing regarding cyber security certification nowadays as seen by ECSO members[3]. On the other hand, the SOTA document gives a good overview of cyber security standards, initiatives and certification schemes, both at the European and international level (including national elements), for assessment and certification of items. One objective of WG1 is to define a comprehensive way to evaluate what can be used (if existing) to address the identified challenges. By comparing the challenges (COTI) with the existing standards (SOTA), gaps in existing standards and

[1] For better readability, we use the term "item" in this document as equivalent for the evaluation of product, system, solution, service, organization.

[2] A vulnerability in software that is unknown to a vendor. This vulnerability is then exploited by hackers before the vendor becomes aware.

[3] Notice, that COTI is a collection of opinions to get an impression where the main challenges are seen. The collection cannot be seen as a consistent, harmonized picture across WG1 members.

certification schemes may be identified as there is no “best” scheme available that fits to every situation or need. It depends on the use case, context and application field. Some schemes are quite efficient because they focus on a fixed use case (e.g. EMVCo [3]) whereas others (e.g. Common Criteria [4]) are designed to be applicable to arbitrary products and thus include extra efforts to fulfil work units which might not be fully relevant for the respective use case at hand. Regarding services and organizations, quite efficient schemes and standards do exist (e.g. PCI DSS, (ISC)[2] certification for professionals) whereas others are quite general (e.g. ISO 27001 and 27002) and are often instantiated for specific domains (ISO 27017 for cloud services, 27019 for energy utility industry). As the market is evolving very quickly and cyber security is pervasive in many vertical sectors, it is unrealistic to define a perfect scheme that fits all needs.

One problem with static certification of products is that the validity of this certification is lost as soon as the first unpatched vulnerability is disclosed. Therefore, certification schemes need to take the patch management into account during a product’s life cycle. In some schemes, this is foreseen in terms of enforced regular re-assessments, but it needs to be ensured that a respective process is lean enough to meet the time to market requirements. It would be convenient to consider a security testing methodology help in the process of updating the certificate[4] in a fast, easy and inexpensive manner. When doing an update or patch, security tests can be executed to assist re-assessment processes and, consequently, for updating the security certificate including the links to any labels or in some cases, the physical label itself. One could also consider having the updating process certified to allow manufacturers in certain cases to quickly react, if a security breach has been found. The process of releasing a new certificate must not hamper fixing an issue and rolling out a patch.

1.1 State-of-the-Art Syllabus

SOTA lists all standards and specifications related to Cybersecurity known to and deemed relevant by the authors at the moment of writing. “Relevant” here means that a standard can (potentially) be used for assessing the security strength of an item.

For each of these standards, the following questions are briefly discussed in the SOTA:

- **Focus**: What is the (main) area of applicability of this standard? (e.g. component, product or multi-product, system, organisation, infrastructure …).
- **Associated Scheme and Governance**: Does a scheme exist to assess, test or certify people, products, services, organizations or infrastructures against this standard? If there is an associated scheme, how is the scheme governed? Who is the Standard Developing Organisation, who is the certification scheme owner? What are the accredited third-party labs, if any?

[4] Remark: the term “certificate” or “security certificate” in this document must not be confused with digital certificates in the sense of Public-Key Infrastructures. In this document by certification we mean the document which a certification body issues, once a security evaluation has been successfully completed and finally the results approved by a certification body.

- **Process:** How does the assessment or certification process work? Is self-declaration allowed, and if yes, how is quality of self-declaration ensured? Are several or different levels of security defined? What do these levels mean?
- **Practice:** Is this standard being used in practice for assessments or certifications? If so, what is the experience and perceived value in the market? How many subjects are certified?
- **Formal Status**: Is there any associated legislation, official mandate or other government involvement?
- **Relation to other standards/schemes**: Is there any official relation with other standards or schemes described in this document?

Remark: SOTA is a living document. This means it will be extended regularly with new identified gaps, new standards or schemes published.

1.2 Challenges of the Industry

The COTI document is a collection of more than 290 inputs or issues to be addressed raised by individual industry members of ECSO WG1. This input addresses a large variety of anticipated problems with the rise of Internet of Things and with the need to cover products/systems to be deployed in the field for many years. A preliminary analysis of the challenges reported by WG1 members reveal that the most recurrent topics include harmonisation, privacy, patching & updating, connected devices, time to market & innovation speed, base line, trusted products and brand protection. The list of challenges below is not to be considered exhaustive. Only the most common ones are reported (here) as they may have a significant impact across several sectors.

Existing schemes are partly mentioned to be “well working” but also facing the issue of **neither being agile nor scalable**, sometimes **expensive** (hundreds of thousands of Euros), **slow** (issuance of certificate months after the product is ready for release) **or too formal** (requiring that everything is perfectly documented to a level which does not add anything further to the security).

SOTA has identified an exhaustive list of standards and certifications available, but when verticals, sectors and product groups are considered there are still many blind spots in some sectors. In general, it is noted that there is a **lack of harmonized requirements** for baseline security for lower assurance levels.

Some schemes include **risk assessment** on the results of the evaluation which works quite well for fixed use cases (e.g. payment) where the risk owner is in place, or at least the direct impact in terms of financial loss is known (e.g. a Bank, Payment Network Operator). Some other schemes like Common Criteria do not include risk assessment in evaluation results as the final usage of the product is not always known. Risk assessment, when considering the supply chain and independent evaluation, is identified as important for liability. Risk assessment has also been mentioned to be key as a starting point to identify the security requirements which have to be fulfilled by the target of evaluation (Remark: depending on the scheme, either risk assessment or threat analysis are the terms used resulting both in a list of security objectives or requirements).

The model of **composite certification** is widely used in the smart card industry, but facing **complexity issues** when it comes to larger products including services, infrastructures and

organizations. It is also criticized that certification might **hamper innovation** as it is only considered a snapshot of the item, taken at the time when the certificate is issued.

Attacks are further evolving and therefore a certificate might give the wrong impression that the product is entirely secure. Just as critical, the need to use certified software might force developers to use older expired versions, as the certification process is not flexible enough to cope with rapid changes and new developments. Another important aspect to be mentioned here is the capability of **patching and updating products securely in the field**. This is essential to keep up with evolving attacks. Certification needs to cope with this efficiently, with either very efficient delta-certifications or by having a certain **degree of freedom within the certified scope**. For example, a set of configurations and adaptations not violating the initial certification, such as configurable countermeasures with different levels of strengths which are reconfigured when attacks happen (or re-configure themselves upon an attack). Another example would be to have the update process certified, allowing manufacturers with higher security maturity level to patch without the need to always re-certify. This might be important to avoid that certification delays the patching and updating of products.

Some inputs are also addressing the issue of **post compromise management**, that is, the situation where a (potentially certified) product is compromised along with the way to manage the attack.

The aspect of **governance** is manifold. Some inputs favour the generalization of the mutual recognition approach of SOG-IS MRA [5] and at the same time clearly indicate that a real **harmonization** is key which is not the case now. To a certain degree industry would expect it: for example, currently, re-use of evaluation evidence between schemes is tough, labs are not working consistently, schemes like CSPN [6] and CPA [7] are only working on national basis.

Privacy is mentioned multiple times, especially in the light of GDPR[5], asking for "**Privacy by Design**" to be considered. Also "**Security by Design**" is mentioned as key to not react only after an incident happens, but having security considered as an integral step in the development process. Certifying the latter is also mentioned to potentially achieve higher security assurance when considering products.

Cheating participants in the supply chain is a rising problem often not properly addressed by certification schemes as it is assumed that vendors follow the processes and are honest during the evaluation. Cheating participants in the supply chain can therefore sell a different product under the certification brand than the one shown to the evaluator during the evaluation process. This requires a proper fix in the supply-chain with e.g. sample checks. This is crucial as otherwise **products with backdoors** can enter the markets, enabling criminals to hack systems.

There are many more challenges mentioned in COTI, but everything mentioned above already shows the variety of industry sector needs. It should also be clear that not all challenges can be addressed by WG1 as some of them are problems of existing schemes or need to be solved outside of standardization or certification, e.g. by regulation.

[5] General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

1.3 Objectives

Considering the COTI and various discussions in WG1 the following key objectives could be drawn for the definition of a future-proof certification methodology[6]:

- **Obj 1.** **Threat analysis** and **risk assessment** shall be the **source to determine security requirements** that are used as the basis for security evaluation & certification of items.
- **Obj 2.** The evaluation of the risk should involve the **risk owner** (e.g. user of a product) and consider the supply chain for **liability**.
- **Obj 3.** A **minimum required baseline** shall be defined against which items are assessed to significantly reduce the deployment of unsecure items (product, services, infrastructure, …) into the European market.
- **Obj 4.** The **burden for manufacturers w.r.t. to certification**, such as bureaucracy, costs, time to market, shall be **minimized** in the context of its usage while ensuring adequate trust in security claims.
- **Obj 5.** Security evaluation & certification shall confirm the **security strength of items** under evaluation against state-of-the art attacks.
- **Obj 6.** **Regular lean re-assessments** shall be part of the governance procedure to reduce the risk of undiscovered vulnerabilities w.r.t. to new attacks that are found in the field; the frequency and methodology should depend on the application field and type (product, service, …).
- **Obj 7.** **Patching** shall be considered as a **standard process** in the certification flow (devices are mostly online in future) rather than as an exception (in the past devices where mostly offline) and shall incorporate delta-assessments.
- **Obj 8.** **Fragmentation** of the market **shall be reduced** by means of **harmonization** while **not reinventing the wheel** (maximum re-use of existing schemes).
- **Obj 9.** **Security by Design** and **Privacy by Design** shall be explicitly taken into account**.**

[6] For simplicity, we do not differ between products, services or organizations here. Some objectives might be more, others less applicable for the respective domain.

2 A META-SCHEME APPROACH

As already indicated in the introduction, several certification schemes exist, but there is no “one size fits all” or silver bullet solution. Moreover, the fragmentation in several markets requires a certain level of harmonization. A composition of existing schemes can be a pragmatic way to combine their advantages while not having to reinvent the wheel. As a starting point a **meta-scheme** can be very useful to

- **Foster trust** by defining transparent rules for certification, including mutual recognition between member states under one umbrella; this requires mechanisms for assuring comparability/adequacy.
- **Harmonize the minimum security required**, agnostic to use cases / verticals.
- **Use and combine existing schemes** (from SOTA) to achieve powerful composition capabilities and harmonization (e.g. by allowing alternative schemes to be used).
- Define a **unified levelling** across use cases / verticals (e.g. to allow the comparison of products of the same category and to standardize the level of assessment applied across verticals).
- Provide a **common way to define the scope & the required security claim (based on risk and threat analysis) especially specific to use cases / verticals**.
- Provide **European Cyber Security Certificates (ECSCs)** for Business-to-Business (B2B), Business-to-Consumer (B2C) and Business-to-Government (B2G) including a **label for simplified understanding especially on the Consumer side**.

By this, not all the challenges identified by the COTI will be solved by a new scheme immediately, but it allows things to be addressed in a consistent way while preserving flexibility for the future and to refine specific aspects of the meta-scheme, such as an according governance model that installs the appropriate orchestration across schemes used under the meta-scheme-umbrella.

In Section 3 we will review aspects of COTI and the objectives listed in Section 1.3 w.r.t. the meta-scheme.

2.1 Indicators of Confidence and Security Strength of an Item

There are schemes like ISO27001 that do not provide any assurance level but a general framework for an organisation to define and describe its information security management system. Various other schemes have different definitions of “levels”. In the simplest form levels express the “level of confidence” or “trust” provided (also referred to as assurance levels). For example, the Common Criteria scheme uses Evaluation Assurance Levels (EALs) 1 up to 7. The higher the level is, the more confidence one can have that what is claimed is fulfilled. This simply comes with the level of **transparency** given to an **accredited third party** that does an assessment.

Generally, on a low level, the assessment approach is rather a black-box (product is used in delivered configuration including publicly available information on the product). Whereas on

higher levels a white-box approach is used (evaluator gets access to source code, design information, open product samples, etc.). Obviously, higher assurance levels are therefore also more expensive. The problem that Common Criteria has is that just mentioning the EAL for a product does not mean anything without mentioning the scope of the evaluation, the security features and security strength. In ISO 27001 certification, a similar problem exists, as the certified Information Security Management Systems may be for a part of the organisation. So, a security claim should be based on risk or threat analysis, resulting in a set of threats and assumptions from which security objectives or security functional requirements and organisational requirements are derived which the item needs to fulfil.

In Common Criteria, for example, it is key to read the so-called Security Target of a product, where at least two dimensions are specified:

- **"What" is evaluated,** that is the part of the item the evaluator will evaluate and can see.
- **"How" it is evaluated,** that is how in depth the evaluator will evaluate the "what" and the level of confidence in the security of the "what" the evaluator will be able to acquire.

It is essential to combine those two aspects as well when defining levels of a meta-scheme.

We propose to require that **with increasing the level of assurance, the scope of security functionality of the item under evaluation must increase**. To avoid a complicated encoding, we recommend having a simple symbol (label) expressing this (e.g. A, B, C, D, E or could be also 1 star up to 5 stars, etc.) (see also Figure 1 and Table 1). The specific meaning and interpretation in detail could be expressed by a diagram which allows more sophisticated encoding especially of the scope of security functionality aspect whilst still being understandable quickly. E.g. a radar-diagram could be used next to the symbol.

We propose to have **two groups** in the security levelling structure (see Figure 1 and Table 1:

- **Base**: items which underwent a sector-agnostic (to a certain extent) standardised base layer evaluation, providing two levels of assurance:
    - **Level E (Entry):** based on self-assessment (done by the vendor) where the minimum scope of security functionality to be fulfilled is basically sector-agnostic and can be seen more as a black-box approach.
    - **Level D (Basic)**: is the same as Entry but with the difference that an accredited third party did the assessment.
- **Advanced**: items which underwent a specific more advanced assessment by an accredited third party with three different levels where the minimum scope of security functionality is sector specific:
    - **Level C (Enhanced Basic)**: assessment depth is starting going beyond a black-box view and the scope of security functionality is sector specific; the assessment requires resistance against an enhanced basic attack potential.

- **Level B (Moderate)**: assessment depth can be considered as a "grey"-box[7] approach and the scope of security functionality is getting clearly higher than for Enhanced; the assessment requires resistance against a moderate attack potential.
- **Level A (High)**: assessment depth is a white-box approach and the scope of security functionality is getting clearly very high; the assessment requires resistance against high attack potential.

Remark: on higher assurance levels, dedicated vulnerability assessment is getting important especially for products. Pure conformity assessment is in several cases not sufficient (e.g. for physical attacks on security ICs).

It shall be noted that an item's scope and depth of security functionality assessed could in principle go beyond the minimum required level. However, for levels in the group "Base" this means the claim gets sector-dependent as the item offers security features that go beyond the sector-agnostic view (see column "Scope of Security Functionality > min" in Table 1).

	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			

Table 1 – Proposal for a Meta-Structure for European Cyber Security Certification.

Into this general levelling structure a static mapping of schemes from SOTA is required (notice we are talking here not only about products, but also about services, organizations, people, …).

Static, in the sense that a table needs to be created where schemes from SOTA can be mapped to the various levels. Sometimes this might be a 1:1 mapping of an entire scheme. Sometimes the levels of a scheme are remapped to the levels of the meta-scheme. This mapping shall not be

[7] The term "grey" is put under quotation marks on purpose. It shall express that it is "something" between black-box (low transparency) and white-box (high transparency).

understood in a way that schemes are considered as equal, if they are mapped to the same level. It just means that they might be used in that level depending on the use case.

Which scheme and how exactly it is subject to the definition in the context of the sector where the levels are instantiated in detail. For example, in the context of e-Government and the use case "Passport" the only allowed scheme will most probably be Common Criteria and the only allowed level will most probably be then "A".

***Disclaimer**:* Table 1 should be seen as a default case/template for sectors. Depending on the sector this might be refined or overridden in exceptional cases where e.g. assessment by a company-internal independent organisation is done for the advanced levels. Notice, however that this can never replace the level of independence and trust which an external party can give. Moreover, for such cases a very strict shadowing process by an accredited third party is required, which tightly audits the internal organisation on a regular basis. This also has an impact on liability. Overriding can also mean that a sector skips the definition of certain levels, i.e. is free to define if and which advanced levels to provide (can be also selective, e.g. only C and A), whereas the basic levels D and E must be supported in any case. It also needs to be noted that there are various opinions on this table, e.g. whether a complete sector agnostic base layer is possible at all or whether there will always be sector-specific things. This needs to be worked out in detail in the next evolution of this document.

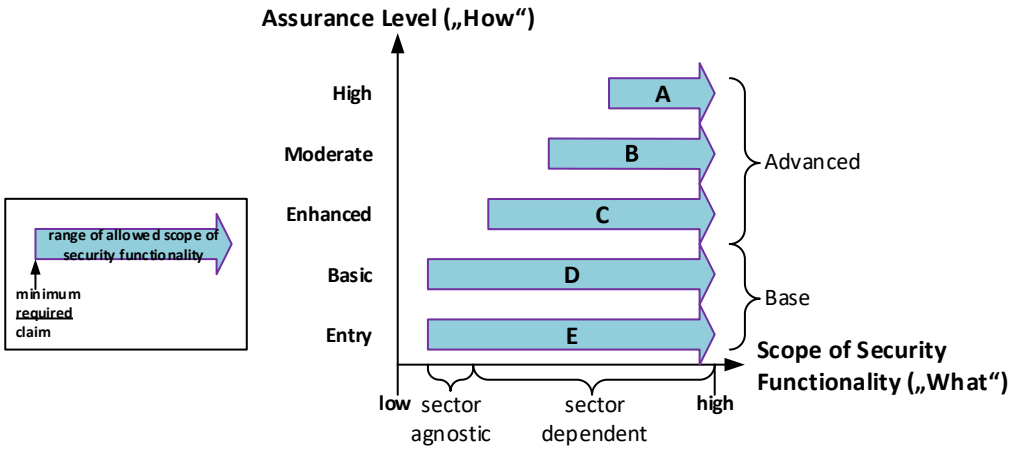

Figure 1 – Correlation between Assurance Level and The scope of Security Functionality.

Figure 1 shows the relation between the Assurance Level and the Scope and depth of Security Functionality assessed. With increasing assurance level the scope of depth of security functionality assessed needs to increase as well. By this we hamper cheating with the levelling scheme by e.g. defining a very narrow scope of security functionality and then assessing the item on assurance level "High" which would finally end up in an "A" which is misleading. As the figure indicates the minimum scope of security functionality for D and E are the same and considered to be sector agnostic. For this part, we recommend to setup a dedicated forum to work out the according threats to cope with and establish a standard against which items need to be assessed to get D or E. In case a higher scope of security functionality is defined, a dedicated sector-specific assessment is potentially required including related risk assessment. For Levels C, B and A the scope and depth of security functionality needs to increase and goes beyond a sector-

agnostic view. Therefore, dedicated expert groups are required per sector, use-case or technology IP.

To allow a simplified understanding on what is covered by an item one could e.g. use radar diagrams similar to that used for showing the features of SLR digital cameras, for example. By this, one can easily see for a product of type X what A, B, C, …, E covers. Figure 2 shows two fictive examples. On the left side, one can see five features defined with their scope of security functionality assessed. When a product is evaluated against the criteria of “Type X” one can choose which level, but then needs to make sure the scope of security functionality is not below the respective claimed line in the radar diagram. The picture on the right shows then a product that claims “B” and as can be seen is covering Features 1-3 on the min. required level for B, but goes far beyond for Features 4-5 (even beyond A for feature 4 from the scope point of view).

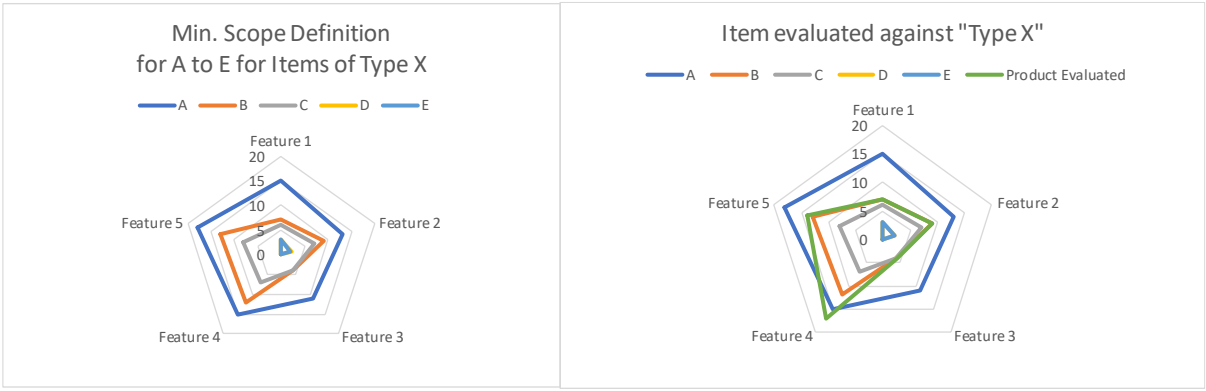

Figure 2 – Example for a Radar-Diagram to visualize Scope of Security Functionality.

Disclaimer: the example of a radar-diagram shall give an understanding that visualization could help a lot to get a feeling on what an item covers. For details in any case one needs to read the details underneath.

2.2 The Role of Expert Groups

Expert Groups (EGs)[8] should be established which select and refine existing schemes (or define new schemes) that focus on advanced security evaluation & certification. The Smart Card industry already did this for Smart Cards and similar devices under SOG-IS [5]. They have set up dedicated groups to define Common Criteria Protection Profiles (which are defining the minimal required set of threats to counter) and creating guidance on the evaluation methodologies (JIL ISCI), an according assessment methodology and attack rating (JIL JHAS) where attack experts (manufacturers, accredited labs, cert. bodies) sit together and maintain a set of state-of-the art attack methods and harmonized quotation. However, as arbitrary devices, components or

[8] In Section 0 EGs fall into the category of “Ad-hoc” groups.

systems get connected in future, this concept needs to scale in terms of security richness, efficiency, cost-effectiveness and flexibility. A meta-scheme can help to start in a pragmatic manner as no new schemes need to be defined at the start, but existing schemes can be combined and interpreted. The interpretation aspect is important as existing schemes do not have an “interface” via which they can be formally combined. Therefore, it is up to the expert group to decide what is sufficient to ensure confidence that required Security and Privacy is provided and what needs to be done on top of what existing schemes cover. For example, one scheme might cover a certain set of attacks (e.g. physical attacks) while another scheme covers another set of attacks (e.g. logical attacks). Requiring both covers then more but there might be still some spots which are neither by one or the other scheme addressed. For those, the expert group may come up with additional required steps for assessment. Notice that most successful cyber security certification schemes focus on small components. Certification of more complex products (e.g. Windows) has not been able to stop the steady flow of attacks on such systems. Therefore, one should realize that certification for complex problems may catch in first glance “low-hanging fruit” attacks, thus, focussing on update and patching processes is very important. The certification of the process for complex systems might be a more suitable approach than the traditional product certification. The latter, however, is key for components and devices.

It is important to not start setting up expert groups for every single use case or technology IP. It needs to be ensured that there is a maximum re-use of what is already existing and this also hold for groups of experts.

Figure 3 shows the types of focus areas Expert Groups may have.

On the one hand the horizontal view is important which is typically the technology IP view. What are the building blocks across sectors (verticals) used? For example, secured micro-controllers will be relevant everywhere and should not be re-certified for every sector. A maximum re-use is key here to save costs for manufacturers, but also to simplify choices when constructing secure ECO-systems. In that case the expert group (mainly technologists and hackers as they understand the technology and the respective threats) is focusing on the technology IP where it is potentially not clear where exactly it is used. Therefore, evaluation results might also yield some tough restrictions for the sake of generality.

On the other hand, there is the vertical view where IP blocks and other aspects are put into a perspective (use case is clear). This also requires dedicated work by an (potentially other) expert group which in that case includes a larger round of stakeholders like customers, risk-owners, hackers, academia, national agencies, labs etc. A dedicated risk assessment can be performed on the evaluation results as the use case is clear and finally a decision may be possible to which kind of residual risks can be taken.

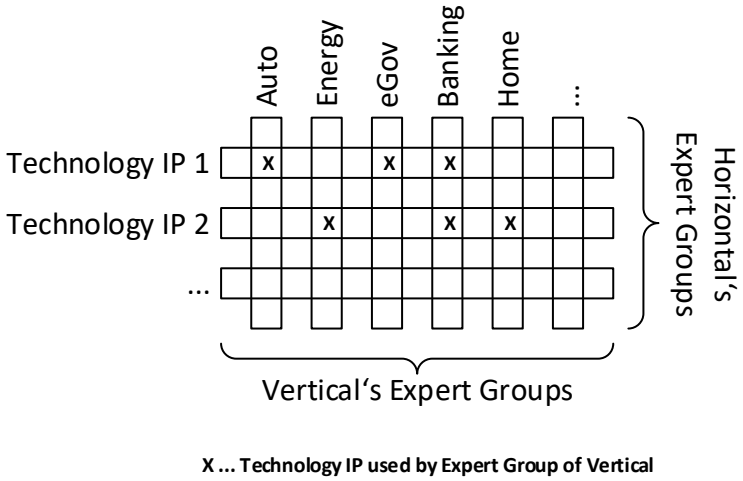

Figure 3 – Different Types of Expert Groups.

2.3 Using a Common Language

When items are evaluated, it is important to understand what the exact **scope of security functionality** is, i.e., the scope evaluated, the threats considered, the assumptions taken, etc. There is no common format to express this across schemes, but such a common format is necessary to be able to combine schemes. Therefore, we recommend to borrow some notion from Common Criteria, slightly modified (see Figure 1).

An expert group defines a **Generalized Protection Profile (GPP)** for the type of item under evaluation. The GPP shall cover the following aspects in a common structured from (a common template):

- **Security Problem Definition** (Threats, Assets, Assumptions, Policies) resulting from risk/threat assessment for the defined scope.
- **Security Objectives**[9] for the item under evaluation and its environment derived from the Security Problem Definition comprising the scope of the security functionality.
- **Security Services and Features** derived from the objectives.
- **Instantiation of the levels** from the Meta-Scheme:
    - The **selection of the schemes** from the static SOTA-mapping and how they are to be applied, i.e. clear definition how results from an existing scheme shall be used to cover certain parts of the scope of security functionality contained in the GPP. This also includes the allowance of alternative usage of schemes (e.g. to

[9] In Common Criteria there are Security Functional Requirements derived from the Security Objectives in a semi-formal form. We do not use this here to stay pragmatic and flexible on the meta-level as the semi-formal language is quite complicated.

meet claim X a certificate of scheme A or scheme B is sufficient if the following aspects are covered: 1 , 2 , 3 …).

- **Visual representation of the minimum required scope of security functionality per level** w.r.t. Security Services & Features (e.g. radar diagram).
- **Additional evaluation** steps required.

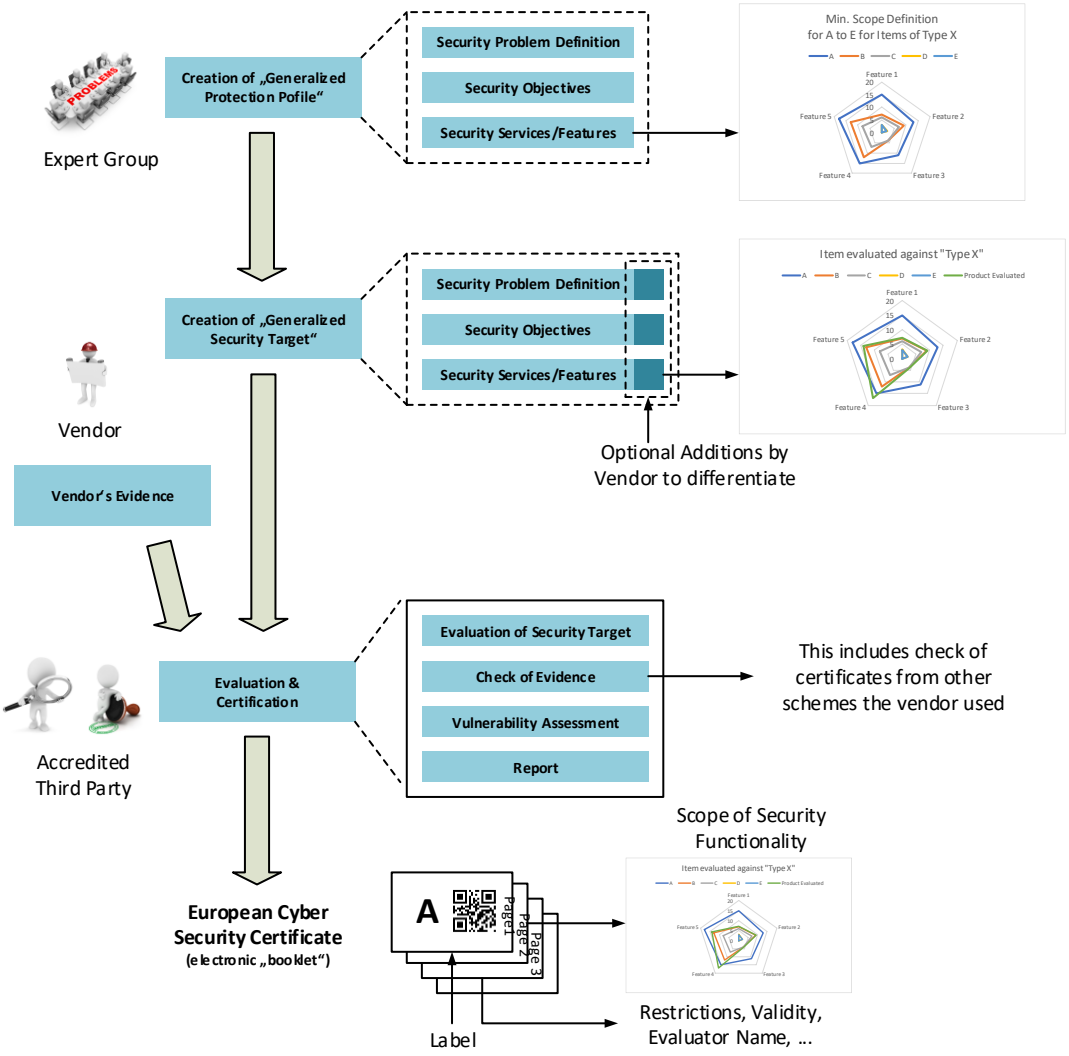

Figure 4 – Meta-Scheme Evaluation & Certification Flow.

The GPP needs to be defined by the respective expert group because it requires deep knowledge about the technical domain, use case as well as threat landscape. Besides that, the Expert Group needs to define potential integration steps as pure usage of results of evaluation from existing schemes is not sufficient. E.g. for more complex products, one could define that the dedicated components of the product are certified by various schemes, where the evaluator checks the consistency of the integration. The trivial case of course is, if there is a 1:1 mapping, e.g. when a product is certified and this certificate just referenced, the GPP would be a translation of the key elements of the respective security claim, protection profile or standard underneath. The evaluator would then just check if the product has a valid certificate and if all assumptions and user guidance restrictions are met.

Remark: the governance of the meta-scheme needs to ensure maximum re-use across sectors is used, i.e. definition of new GPPs shall be approved centrally, also to make sure the right level of granularity is preserved (see Section 4).

Next to the GPP-Template the meta-scheme shall also provide a template of a **Generalized Security Target (GST)**. The term "Security Target" is again borrowed from the Common Criteria Standard. The GST needs to contain the following:

- **Reference to the GPP** which is used as a basis for evaluation and definition/selection of parts which were left open by the GPP (i.e. some parts require instantiation).
- **Additional claims** which are specific to the item under evaluation (this the vendor might want to use to differentiate from other vendors).
- **Key security features and services** fulfilling the claims (this might include additional ones compared to the GPP).
- **Visual representation of the claims** (GPP + GST in combination).

For the security features & services it is recommended to support trustworthiness by item-inherent security characteristic. The meta-scheme shall encourage this throughout the governance structure.

Similarly, the certificate and result of the certification (report) should be translated into a unified format as well: the **European Cyber Security Certificate (ECSC)**. The ECSC can be considered as an electronic booklet containing several aspects (which are in other schemes often covered by two documents: certification and report):

- **Label** (A, B, …) including e.g. a QR-code or NFC-tag for navigation to an online[10] version of the ECSC.
- **Main attributes of the evaluation** such the exact name of the product, sector identifier, unique identification of GPP, GST, the Accredited Third Party used, validity of certificate, list of guidance documentation evaluated, evaluated configuration options, etc.
- **Scope of Security Functionality** and respective evaluation results in simple visual form (e.g. radar diagram).
- **List of subsequent certificates** used (be it ECSC or others).

The ECSC shall be structured in a form that it can be used for end products (like consumer products) but also for developers in the supply chain. The end user might only be interested in the first 2 pages where the claim and the basic attributes are described in simple form whereas the developer needs to consider a very detailed view of the scope of security functionality, the restrictions and the associated guidance.

The GPP needs to be approved by an Accredited Third Party of the meta-scheme. This needs to be defined in the governance structure as it is important to have a certain level of quality

[10] Depending on the use case this might not be always the case

preserved across verticals and horizontals. Likewise, as GPP is worked out by expert groups the logical consequence is that for levels D and E in their minimal required form there should be ideally one GPP with some options included for slight differences across use cases, whereas for A, B, C several GPPs exist (and potentially also for D and E if the scope of security functionality is bigger).

2.4 Examples for combining schemes

In the following, examples are given to show the richness of the cascading-approach. Thereby, the notation from Figure 5 is used to encode different types of schemes: green relates to the certification of services, orange to the certification of organizations resp. sites and blue to products. A red frame means that everything within that frame is covered in an ECSC. The "boxing" shall illustrate the composition of different aspects. For example, a blue box having an orange box embedded means that a product shall be certified w.r.t. the mentioned product certification scheme where e.g. the site of the respective manufacturer needs to be certified according to a certain organizational certification scheme.

Figure 5 – Notation.

Disclaimer: these are just artificial examples for illustration. Further examples need to be added here to illustrate the applicability in various verticals.

2.4.1 Example 1: A consumer product

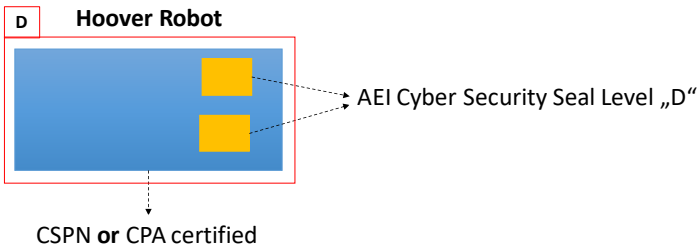

Figure 6 – Hoover Robot Certification.

Figure 6 shows a consumer product which is certified either with the CSPN scheme [6] under ANSSI (France) or with the CPA scheme [7] under CESG (UK). The organisation developing the robot has an AEI Cyber Security Seal Level "D" [8]. The robot itself could be finally classified e.g. as D.

Notice, the example does not mean that CSPN and CPA can be considered as equal, but the respective expert group can define that the required level for the robot is sufficiently considered by both schemes and hence both are accepted equally *for this use case*.

2.4.2 Example 2: Combination of several schemes for product, service and organisation

Disclaimer: This paragraph is an illustration. Expert groups will define verticals and specific areas of the requirements to be fulfilled to achieve each ECSC levels.

Figure 7 shows a cloud service composed of the cloud storage service itself, service being delivered to customers (B2B and B2C), and a Security Operation Center (SOC) that supervises the security of the cloud network. The full cloud service (including SOC) has an ECSC level C certificate. The cloud service itself is certified ECSC level B and the external SOC service is certified ECSC level C.

To be ECSC level B, the cloud service has got an accreditation SecNumCloud level 1. The security network architecture and its configuration has been audited and penetration tested by a lab having a PASSI approval. People operating the service have been CISSP certified. The architecture of the cloud network has ECSC certified devices, for example ECSC level D routers, ECSC level A firewalls, ECSC level E servers and workstations, …

To be ECSC level C, the SOC service is certified AEI cyber security seal level B, and can have similar constraints on its network architecture than the ones of the cloud network.

As can be seen from the box colouring we have a mix of product, service and organization certifications all combined under the meta-scheme resulting in ECSCs: one for the Cloud-Storage Service which has subsequent ECSCs for the Server Center.

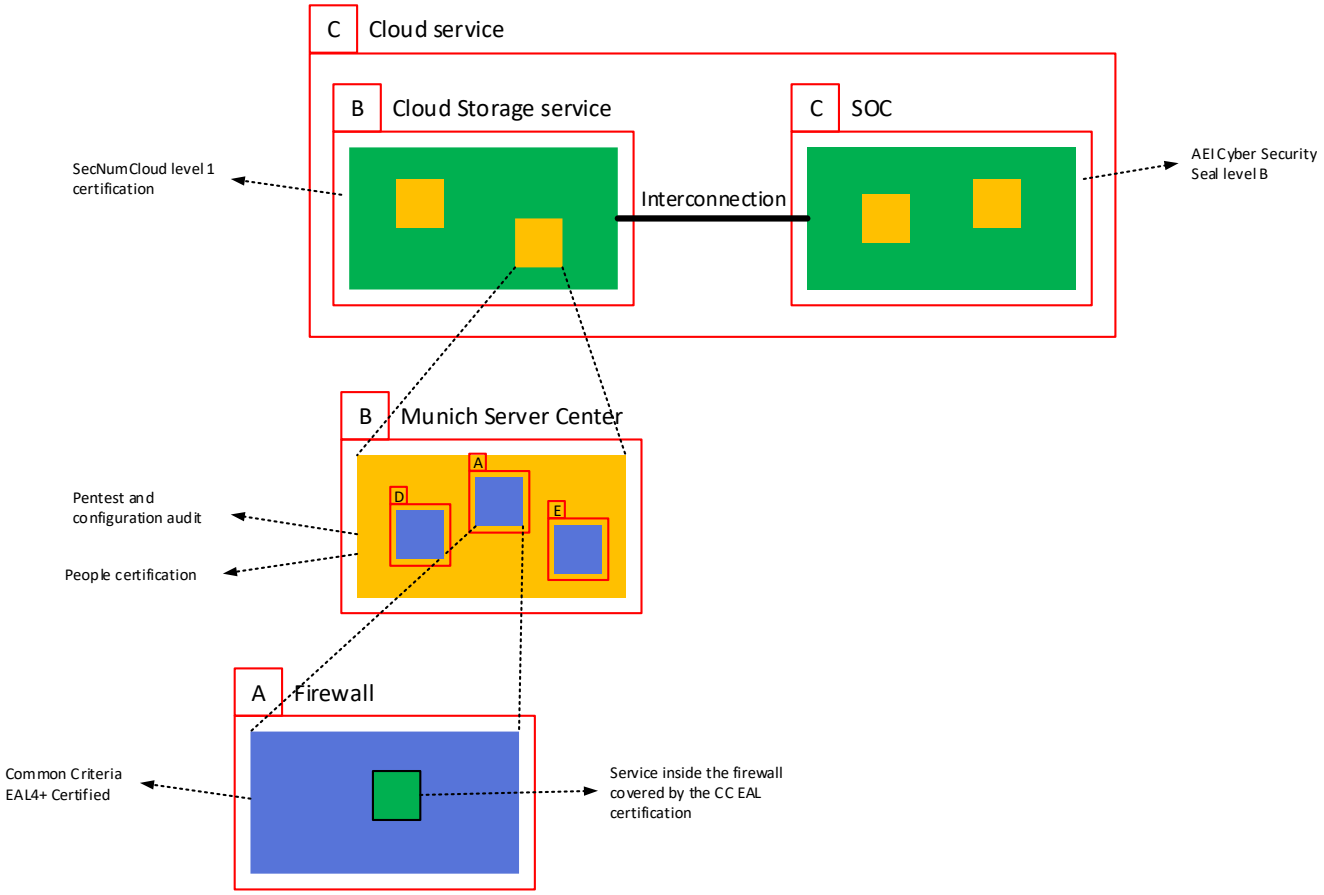

Figure 7 – Cloud Storage Service Certification.

2.4.3 Example 3: Access Control Card Evaluation

Example 3 shows the flexibility, if alternative schemes are allowed. For example, EMVCo IC evaluation [3] and Common Criteria Security IC Protection Profile [9] have a big overlap in the scope and claim as well as the attack methodology used. If the product at hand is exactly matching this overlap one could give the freedom of choice to show either an EMVCo or Common Criteria certificate. The same is valid for the Operating System [10]. On the top-level (e.g. an Access Control Card) one could define proprietary assessment steps tailored to the Use-Case including e.g. the AEI cyber security seal level “D” [8].

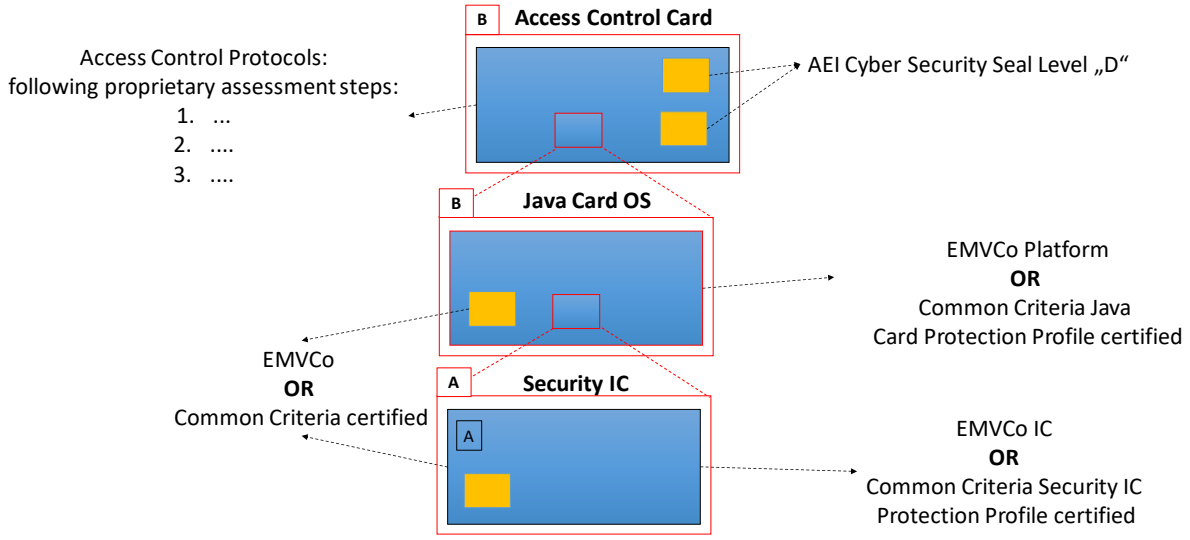

Figure 8 – Access Control Card Certification.

2.4.4 Example 4: Cloud Service Provider

Figure 9 shows a cloud service provider that offers two cloud services: Cloud Storage and Infrastructure. The Cloud Storage Service has a rating level B of LEET Security and the Infrastructure Service has a rating level C of LEET Security. The provider as a company, holds an ISO/IEC 27001 certification that includes previous services in the scope. The company as a whole has an ECSC level C certificate. The cloud storage service itself is a certified ECSC level B and the IaaS is a certified ECSC level C.

As to be seen from the box colouring there is a mix of product, service and organization certification all combined under the meta-scheme resulting in different ECSCs: one for each cloud service provided (Cloud Storage and IaaS), another for the product (firewall) and, finally, another for the company as whole.

This gives the possibility of each service having its own security level, so it could adhere to the needs of the expected users: Cloud Storage is envisioned for clients with higher security requirements (level B) than IaaS (level C) which at the ends provides more efficiency as security requirements are better matched with security features implemented and certified by services.

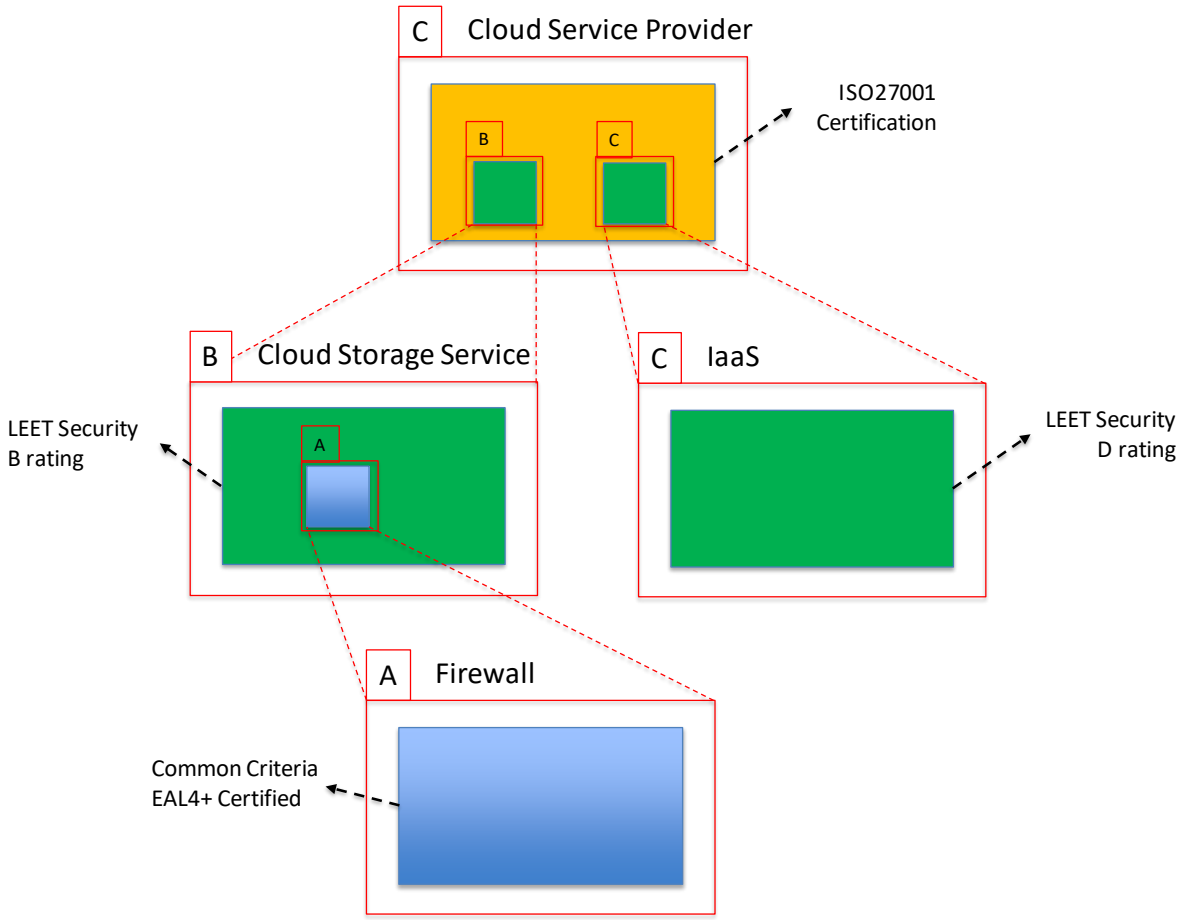

Figure 9 – Cloud Service Certification.

3 MAPPING COTI AND SOTA TO THE META-SCHEME LEVELLING STRUCTURE

Figure 10 illustrates the mapping principle between COTI, SOTA and the levelling structure of the meta-scheme. Some parts of COTI are to be addressed in the meta-scheme itself. These include but are not limited to:

- **Harmonization**: the meta-scheme allows the definition of alternative choices across schemes. Furthermore, the meta-scheme defines a base layer as an entry point for base harmonization. This partially covers Obj 3 and Obj 8.
- **Risk assessment on meta-level**: on the one end for the selection of threats, but also for the assessment on residual risks of the evaluation results performed by risk-owners. This partially covers Obj 1 and Obj 2.
- Levelling implements **increasing scope of security functionality with increasing security assurance**: the levels in the meta-scheme are combining security assurance and the scope of security functionality and mandate the scope to increase with the level assurance increase. This covers Obj 5.
- **Composition with a certain degree of freedom**: schemes from SOTA can be combined where the “combination” step is kept pragmatic (avoiding to much burden of bureaucracy at least on meta-level), where the expert group of the sector/vertical/horizontal can define, under which conditions results from other schemes are accepted and which additional steps need to be performed (e.g. with feature interaction between components). This partially covers Obj 4 and Obj 8.
- **Security & privacy by design**: the meta-scheme allows arbitrary combination; this also also means schemes that are focusing on processes to achieve high maturity levels for security by design and privacy by design. The respective expert group can mandate such process certifications. In the definition of the base layer this can also be mandated via a GPP. There is no dedicated objective, but this addresses the mentioned COTI input.
- **Patching**: assurance practices rules for patching and the enforcement of regular reassessments can be defined by expert groups; of course, it needs to be ensured that a common quality level is preserved across groups, but this can be solved via the governance structure. There are several ways possible, i.e. having it part of the certification procedure to assess patches in a delta-certification or certifying the process of the manufacturer to have an according vulnerability management system used. This depends on the situation. This partially covers objectives Obj 6 and Obj 7.

Other parts (there is also an overlap of course with the meta-level) of COTI are topics to be addressed in the schemes used from SOTA as those were criticized due to experiences with existing schemes. Those include for example: complexity issues in composite certifications, time to market, costs or formalisms. Notice, that many of the topics do not necessarily mean that the standard underlying an existing scheme is bad. Very often the governance structure adds complexity. But this needs to be analysed in detail and improvement proposals made as a next step.

SOTA itself needs to be mapped to the levels in the meta-scheme. Thereby, in a static form first to show which schemes are in principle “allowed” in each level for the different types of certification (products, systems, solutions, services, etc.). How each scheme is to be applied needs to be defined by the respective expert groups. The mapping process needs to be consistent across all use cases, which the according governance structure needs to cope with. It is also clear that SOTA mappings cannot solve all challenges. The respective gaps need to be identified and either be addressed by the expert groups as separate steps to be taken and defined in GPPs, or existing schemes need to be extended or some new schemes defined under the meta-scheme.

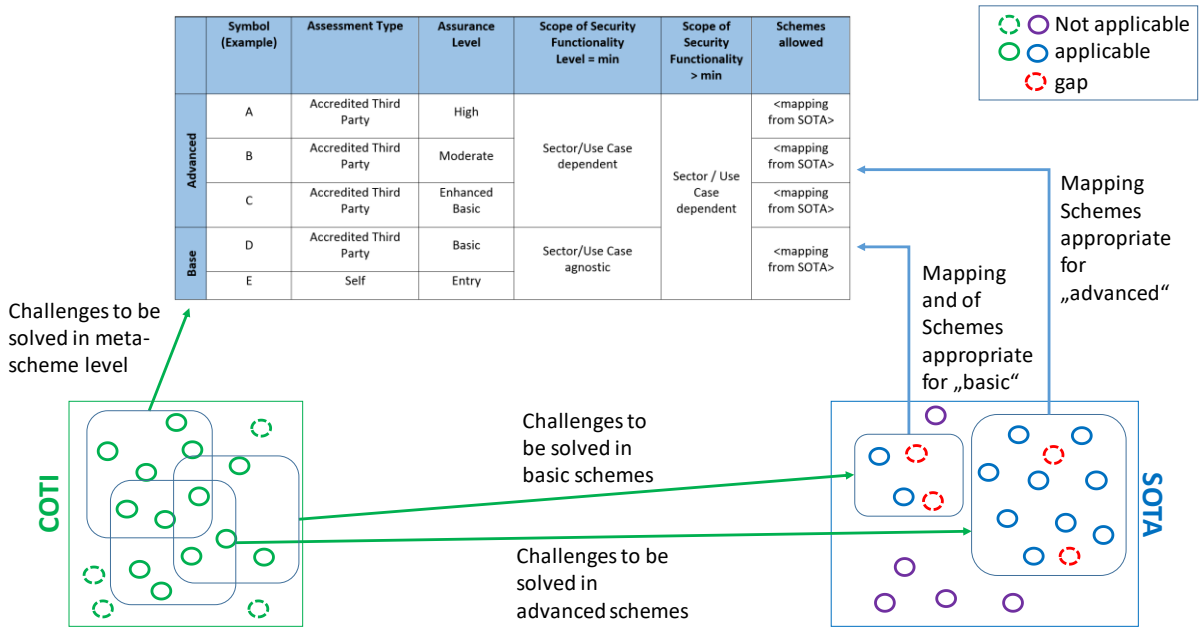

Figure 10 – Mapping of SOTA and COTI.

4 GOVERNANCE STRUCTURE

Disclaimer: two governance models have been proposed in WG1 and first discussions took place in the WG1 meeting on 31.8.2017. On 13.9.2017 the European Commission published the proposal for a Regulation on ENISA and on the ICT cybersecurity certification. As the two proposed governance models and the direction of the Commission are quite diverging we see the necessity to further discuss the governance expectations from Industry within WG1 before coming up with a consolidated view. As a start, we list the following minimal set of expectations from such a governing structure:

1. Governance shall ensure that **bureaucracy is minimal**, certification is **cost-efficient** and **time-to-market** is put into the center of focus while **not putting security quality at risk** (see also Obj 4 and Obj 5). Adequate balance between both questions (time to market vs. security quality) must be the most relevant goal for the new Meta framework in Europe. The concern about the current low speed of CC certification processes and that any increase on the scope or level of security required to ICT products over Europe may produce are a real concern for the Industry, and are the main reasons behind the fact that little percentage of ICT products receive any kind of security screening.
2. Governance shall ensure that **patching is considered as a standard process** in the certification flow (see also Obj 7)
3. Governance shall ensure that **sector-specific security requirements and evaluation & certification procedures** are optimized by a **dedicated Expert Group (EG)**, which consists of, but is not limited to, representatives from Industry, security experts, national security agencies, regulators and evaluation bodies and certification bodies. A real concern coming from the Industry is the possibility of having only public sector oriented producers of requirements, that can produce a disruption as much as only private sector groups, can do. A good balance between all members, will produce trust on Expert Groups.
4. Governance shall ensure that the **Expert Group for a sector is operating to a certain level of quality**, i.e. it must not happen that a set of stakeholders that have little experience in security define a setup that damages the reputation of the entire meta-scheme (e.g. “cheaters”).
5. Governance shall ensure that there is a **maximum re-use of certified items across sectors**, i.e. a central body needs to ensure sectors are not re-inventing things.
6. Independent Certification Bodies are paramount on getting time to market capacity on any Meta framework, although governance shall ensure that **evaluation & certification bodies** are working on a mutually **consistent quality level**. The role of accreditation of independent certification bodies, must be done by a security expert national body, instead of standard accreditation bodies, since the capacity of evaluating the maturity level of those bodies, requires specific knowledge and expertise.
7. Governance shall ensure that **cheating participants are blacklisted if detected**, that is e.g. manufacturers selling a non-certified product along with a certificate from another one (that differs only in a configuration, for instance).

5 CENTRAL REPOSITORY FOR GENERALISED PROTECTION PROFILES, SECURITY TARGETS AND CERTIFICATES

To provide trust, transparency and efficiency it is required to install a central service which could offer the following functionalities (list is not exhaustive):

- Authentic storage[11] of **Generalized Protection Profiles, Generalized Security Targets** and respective **European Cyber Security Certificates** matching the GSTs.
- Storage of **certificates from other schemes** (from SOTA) where possible.
- **Notifications** on expirations, renewed and updates versions, changes, revocations, etc.
- **Search engine** to efficiently find items and related certificates.

With such a central data base the status of a product, organization or service can be checked and traced. This is crucial as attacks evolve over time and the certificate needs to be dynamic and therefore maintained in electronic form. For convenience, certified items could be e.g. equipped with a QR-code or NFC tag which allows fast online checking of the certificate's status.

One issue which a database could help with, is to detect cheaters. Integrity & authenticity throughout the production and supply chain are crucial. How can a user know that the product at hand is really the certified one? If vendors in the supply chain are honest, it works. But e.g. if the HW manufacturer produces a different device than certified, it is hard to detect (it might be even only some configuration that differs). A database alone is not sufficient, but could store reference information for detection.

Remark: creating such a database is not trivial as especially the information from other schemes is potentially out of control. Moreover, it needs to be clearly defined who owns, runs and pays for the maintenance of such a database. This strongly depends on the governance structure and funding around the meta-scheme.

[11] There might be cases where Certificates are kept secret and therefore not stored on the database.

6 CONCLUSION

The work of ECSO WG1 up to now resulted in two documents (COTI and SOTA), which act as a good basis to understand the challenges ahead as well as the state-of-the art to identify gaps towards a harmonised European certification framework. To not reinvent the wheel, a meta-scheme should be established that allows combining existing schemes efficiently or to allow creation of new schemes when required.

A definition of **Generalized Protection Profiles (GPPs), Generalized Security Target (GSTs)** and **European Cyber Security Certificates (ECSCs)** allows a simple unified understanding on the one hand for consumers, but also provides sophisticated details to allow products in the supply chain to be used under certified conditions. A central database storing templates and certificates allows efficient navigation and notification capabilities.

It is clear, that a meta-scheme will not solve all the challenges mentioned in COTI, but it allows to address the challenges common to most of vertical sectors and stay flexible for tailoring certification towards use cases for different markets. The silver bullet is in reach. Any kind of gaps seen in existing schemes that are still comparably the best choice requires an optimization of that scheme. The expert groups, mixing experience from vertical segments and horizontal technology domains, will be instrumental to achieve a proper application of the meta-scheme across markets. For instance, Common Criteria is always criticized for its formalisms, complexity, high costs and bad time-to-market figures. However, to a large extend this is not a problem of the standard itself, but an issue of how it is applied including the governance around. There is also clearly a lack for the Basic layer. This is also the area where the highest focus should be set once the meta-structure is finalized.

7 GLOSSARY

Acronym	Definition
(European Cyber Security) Meta-Scheme	Certification scheme that allows to combine other schemes
Accreditation	Formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards (Source [11], definition 3.2). Third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment results (Source: [12], definition 5.6).
Accredited Third Party	Legal entity different from vendor or purchaser.
Asset	Anything that has value to an individual, an organization or a government results (Source [13]).
B2B	Business-to-Business.
B2C	Business-to-Consumer.
B2G	Business-to-Government.
CB	Certification Body.
Certification	Third-party attestation related to products, processes, systems or persons. NOTE: Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable. (Source [12], definition 5.5).
COTI	Challenges of the Industry.
ECSO	European Cyber Security Organisation.
European Cyber Security Certificate (ECSC)	Booklet summarizing the results of an evaluation of an item. This includes a label, basic attributes like name of product, GPP and GST used, restrictions of the usage, simplified encoding of the claim in visual form, etc.
Evaluation	Assessment of a deliverable (document, item, entity) against defined criteria (Note: extended form ISO/IEC 15408-1:2009 [4]) systematic determination of the extent to which an entity meets its specified criteria (Source [14], definition 4.12).
Expert Group (EG)	Group of stakeholders defining security requirements and assessment methodologies; this can be a set of customers, vendors, risk owners, hackers, labs, national agencies, etc.

Generalized Protection Profile (GPP)	Document describing the minimal security claim an item of a certain type needs to fulfil.
Generalized Security Target (GST)	Document describing the exact security claim that an item at hand needs to fulfil.
Horizontal	Technology domain, IP; building blocks for products, systems, solutions.
ISCI WG1	International Smartcard Certification Initiative - Working Group 1.
Item	Product, service, system, solution, organization, process that is certified.
JHAS	JIL Hardware-related Attacks Subgroup.
JIL	Joint Interpretation Library.
Label	Symbol encoding the certification class/level reached (e.g. A, B, ..., or 1, 2, 3, …) used for marketing purposes.
Risk	Potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [15].
Risk Analysis	Process (2.61) to comprehend the nature of risk (2.68) and to determine the level of risk (2.44) (Source [16], 3.6.1) Process of identifying security risks, determining their magnitude and identifying areas needing safeguards [15].
Risk Evaluation	Process (2.61) of comparing the results of risk analysis (2.70) with risk criteria (2.73) to determine whether the risk (2.68) and/or its magnitude is acceptable or tolerable (Source [16], 3.7.1).
Risk Identification	Process (2.61) of finding, recognizing and describing risks (2.68) (Source [16], 3.5.1). Note 1 to entry: Risk identification involves the identification of risk sources, events (2.25), their causes and their potential consequences (2.14).
Risk Assessment	Process used to identify threats to counter with an item overall process (2.61) of risk identification (2.75), risk analysis (2.70) and risk evaluation (2.74) (Source [16], 3.4.1).

Risk Treatment	Process of selection and implementation of options to modify risk [16]. Risk treatment can involve the following: • avoiding the risk (2.68) by deciding not to start or continue with the activity that gives rise to the risk (2.68); • taking or increasing risk (2.68) in order to pursue an opportunity; • removing the risk (2.68) source; • changing the likelihood (2.45); • changing the consequences (2.14); • sharing the risk (2.68) with another party or parties (including contracts and risk financing); • retaining the risk (2.68) by informed choice.
Security Strength Claim	It refers to system property relative to demonstration of the ability of: a) detecting, reacting or tolerating perturbations (even from malicious actor) that might affect the entity or system's behaviour and b) keeping persistence of entity or system's characteristics after perturbation.
Sector, Vertical	Market use case where building blocks from the horizontals are used to compose a solution.
SOTA	State of the Art Syllabus
Vulnerability Assessment	Is the process which an evaluator performs when evaluating the item at hand to see whether there are spots to exploit for an attack.

8 REFERENCES

[1] European Cyber Security Organisation (ECSO) WG1, *Challenges of the Industry. Internal document,* Brussels, 2017.

[2] European Cyber Security Organisation (ECSO) WG1, *State-of-the-Art Syllabus: Overview of existing Cybersecurity standards and certification schemes v2.0,* Brussels, December 2017.

[3] EMVCo, "Security Evaluation," [Online]. Available: http://www.emvco.com/approvals.aspx?id=31. [Accessed December 2017].

[4] ISO/IEC 15408, "Information technology -- Security techniques -- Evaluation criteria for IT security," 2009.

[5] SOG-IS -- Security, Senior Officials Group Information Systems, [Online]. Available: http://www.sogis.org/.

[6] ANSSI, "Certification de Securite de Premier Niveau (CSPN)," 2008. [Online]. Available: https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-centres-devaluation/. [Accessed December 2017].

[7] CESG, "Commercial Product Assurance (CPA)," [Online]. Available: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa. [Accessed December 2017].

[8] AEI Ciberseguridad. Cluster, Spanish Cyber Security, "Certification Seal of Cybersecurity for Organizations," [Online]. Available: https://www.aeiciberseguridad.es/index.php/Sello_AEI. [Accessed December 2017].

[9] *Security IC Platform Protection Profile with Augmentation Packages Version 1.0. BSI-CC-PP-0084-2014.,* 2014.

[10] *Java Card Protection Profile - Open Configuration ANSSI-CC-PP-2010/03-M01.*

[11] ISO/IEC 21827, "Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model," 2008.

[12] ISO/IEC 17000, "Conformity assessment -- Vocabulary and general principles," 2004.

[13] ISO/IEC 27000, "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary," 2016.

[14] ISO/IEC 12207, "Systems and software engineering -- Software life cycle processes," 2008.

[15] ISO/IEC TR 13335-1, "Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security," 1996.

[16] ISO Guide 73, “Risk management -- Vocabulary,” 2009.

[17] ITU-T X.1252, “Baseline identity management terms and definitions,” 2010.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU