European Cyber Security Certification

Product Certification Composition

WG1 – Standardisation, certification and supply chain management

November 2020

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

Copyright Notice

Executive summary

Until recently, security certification applied to a limited type of processes and products. Schemes have been defined for each product or process category, which have often become more and more complex over time. A similar scenario now appears in many fields, as complexity increases. Cloud-based systems, IoT deployments in factories or in cities, and even cars, are now so complex that a global certification can only be achieved by assembling certified components. Composition is the generic name for this assembly process.

Composition applied to certifications naturally springs to mind when building a product from previously certified components. When a product is built by assembling components, the objective is to reuse as much as possible the evidence and the results that come with the certified component during the evaluation of the composed product.

This document addresses product certification composition with the objective to analyse what are the conditions and procedures when seeking a certification by composition under the requirements defined by EU Cybersecurity Act. The goal is to *focus on composition in an agnostic way with respect to the standards and the certification schemes*, targeting the value of the composition to decrease time to market and certification costs while maximising assurance for multi component products.

The document provides high level guidelines for product certification composition, highlighting the importance to perform certification composition beyond the traditional single scheme.

A generic Internet of Things (IoT) device is used as a reference study case to illustrate the guidelines for the product certification composition in practice.

A second document release is planned to provide more technical details and a practical approach for scheme composition with the first European certification schemes.

Table of Contents

1 Objectives

The objective of this report is to provide guidelines and structure how to proceed when seeking a certification by composition under the requirements defined by EU Cybersecurity Act (regulation (EU) 2019/881 of the European parliament and of the council of 17/04/19) [1].

The aim is not to define a new certification scheme or propose a new standard to support composite certification and the evaluation of products under a certification by composition. **The goal of this analysis is to produce standard agnostic conditions and guidelines to achieve cybersecurity certification composition**. In this context, a mix of different standards is considered when building up the targeted product.

This report does not focus on the assessment rules nor how to perform the assessment; this topic is discussed in the ECSO Assessment Option document [2].

The guidelines for the product certification composition will be illustrated on a generic Internet of Things (IoT) device.

The document is structured as follows. Section 2 and 3 present the terminology and definitions used in this document and a brief reprise of the Cybersecurity Act. Section 4 discusses the need for product certification composition and sets the perimeter of the problem addressed in this report. Section 5 analyses the factors that need to be considered to enable the composition. Section 6 defines the guidelines for certification composition. Finally, Section 7 introduces the reference study case analysed for composition in practice and Section 8 draws together some concluding remarks.

2 Glossary

The definitions reported hereafter integrate those taken from ECSO Glossary document. Some terms have been refined in accordance to the Cybersecurity Act [1] and to the context. In such case all applicable definitions are reported.

Term	Explanation/definition
Accreditation	Def. #1: Third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks. Def. #2: Attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonized standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.
Accreditation body	Authoritative body that performs accreditation.
Assurance level	"'Assurance level' means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned" (source: Cybersecurity Act [1]).
Attestation	Issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated.
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf. Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011 [3].
Certification	Third-party attestation related to products, processes, systems or persons. For instance, a cybersecurity certificate under the European Cybersecurity Act means a document issued by a relevant certification body, "attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme." (source: Cybersecurity Act [1]).
Certification body	Third-party conformity assessment body operating certification schemes. A certification body can be non-governmental or governmental (with or without regulatory authority). For instance, in the framework of the Cybersecurity Act, a certification body is the entity issuing the certificate.

Term	Explanation/definition
Certification scheme	Certification system (Conformity assessment system) related to specified products, to which the same specified requirements, specific rules and procedures apply. A “certification system” is a “conformity assessment system”, which is defined in ISO/IEC 17000 [4]. In this document a certification scheme refers to the “European cybersecurity certification scheme” defined in the Cybersecurity Act [1].
Conformity	Fulfilment of a requirement.
Conformity assessment	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.
Conformity assessment body	Def. #1 (ISO/IEC 17000 [4]): Body that performs conformity assessment services. Def. #2 (Regulation 765/2008 [5]): Body that performs conformity assessment activities including calibration, testing, certification and inspection.
Conformity assessment scheme	Conformity assessment system related to specified objects of conformity assessment, to which the same specified requirements, specific rules and procedures apply.
Conformity assessment system	Rules, procedures and management for carrying out conformity assessment.
Conformity self-assessment’	“’Conformity self-assessment’ means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.” (source: Cybersecurity Act [1])
Evaluation	Def. #1: Combination of the selection and determination functions (sampling, testing, inspection, review) of conformity assessment activities. Def. #2: Assessment of an IT product or a Security Profile against the IT security evaluation criteria and IT security evaluation methods to determine whether or not the claims made are justified.
Evaluation authority	Body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements ISO/IEC 15408 [6] for that community by means of an evaluation scheme.
Evaluation scheme	Administrative and regulatory framework under which ISO/IEC 15408 [6] is applied by an evaluation authority within a specific community
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.
Multi-assurance evaluation	Evaluation of a TOE using a Security Profile where each component evaluated under the Security Profile is associated with its own set of assurance requirements. Note 1 to entry: At least one of the components evaluated under a Security Profile contains a different set of assurance requirements to the others.

Term	Explanation/definition
Process	Set of interrelated or interacting activities which transforms inputs into outputs.
Requirement	Need or expectation that is stated, generally implied or obligatory. Note 1 to entry: “Generally implied” means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example in documented information.
Residual risk	Risk remaining after risk treatment Note 1 to entry: Residual risk can contain unidentified risk. Note 2 to entry: Residual risk can also be referred to as “retained risk”.
Review	Def. #1: Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Def. #2: Verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements by an object of conformity assessment.
Risk	Effect of uncertainty on objectives. Note 1 to entry: An effect is a deviation from the expected — positive or negative. Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Note 3 to entry: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73 [7], 3.5.1.3) and “consequences” (as defined in ISO Guide 73 [7], 3.6.1.3), or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73 [7], 3.6.1.1) of occurrence. Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.
Security Profile (SP)	Implementation-independent statement of security needs for a type of ICT product / Target OF Evaluation. This is also called a Protection Profile under the Common Criteria scheme but adds a risk-based approach in identifying and selecting the security requirements. More specifically, a Security Profile (SP) addresses a specific problem definition while considering the type and sensitivity of assets and the context of the operational environment (e.g. Consumer, Enterprise, Industrial) and the risk factor. A SP

Term	Explanation/definition
	contains a summary of the security requirements that must be covered by the TOE Security Functionality. Its definition is a step towards an economic way of dealing with security evaluation. It helps to scale security controls and security-related process activities in accordance to the identified risks, i.e. to spend most effort where the highest risks are. Security Profiles may be agreed on and standardised for certain product classes. A standardised security profile saves a detailed risk analysis for every new product instance. It provides an accepted standard on security properties of a product.
Security Target (ST)	Implementation-dependent statement of security needs and security functionalities for a specific identified Target Of Evaluation (TOE).
Specified requirements	Need or expectation that is stated. Specified requirements may be stated in normative documents such as regulations, standards and technical specifications.
Statement of compatibility	This concept identifies under which conditions the composite product can trust in and rely on the security functionalities of the certified component without re-evaluating them. For instance, this could be defined based on public information describing the security functionalities of the certified component.
Testing	Determination of one or more characteristics of an object of conformity assessment, according to a procedure.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organization.
TOE	Target of Evaluation.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

3 EU Cybersecurity act requirements

3.1 Security Objectives

This report will not define any security objective for its analysis, as it is considered that any component and product, going through certification under a scheme that is compliant with the EU Cybersecurity Act, will follow the security objectives as defined in article 51 of the EU regulation 2019/881 [1].

3.2 Assurance levels

The Assurance levels for this report will follow what article 52 of the EU Cybersecurity Act states and will remain at product level, not addressing at this stage its ecosystem.

The Cybersecurity Act (regulation (EU) 2019/881 of the European parliament and of the council of 17/04/19) [1] assurance levels are as following:

*1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: **'basic', 'substantial' or 'high'**. The assurance level shall be commensurate with the **level of the risk** associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.*

2. European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme under which the European cybersecurity certificate or EU statement of conformity is issued.

*3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding **rigour and depth** of the evaluation that the ICT product, ICT service or ICT process is to undergo.*

4. The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.

*5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level '**basic'** shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the **known basic risks of incidents and cyberattacks**. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.*

*6. A European cybersecurity certificate that refers to assurance level '**substantial'** shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of*

*incidents and **cyberattacks carried out by actors with limited skills and resources**. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.*

*7. A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of **state-of- the-art cyberattacks carried out by actors with significant skills and resources**. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.*

*8. A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an **appropriate combination of assurance components**.*

3.3Elements of cybersecurity certification schemes

The Cybersecurity Act (regulation (EU) 2019/881 of the European Parliament and of the Council of 17/04/19) [1] defines the elements to be included in the certification scheme in Article 54. The article is available for reference in the Annex 1. The elements under consideration for enabling composition are discussed below.

- The scope of the certification scheme should include the possibility to allow for the reuse of evidence, the type of categories covered by the evidence reused and to what extent (partial or full). The scheme should indicate whether composition reusing evidence certified in a different scheme is allowed (Article 54.1.a).
- The purpose of the scheme should allow for composition, in particular for the evaluation methods and the assurance levels attained, or if there are any restrictions defined by the certification scheme (Article 54.1.b).
- The rationale to attain an assurance level in case of composition could be part of the definition of the certification scheme (Article 54.1.d).
- The evaluation criteria and methods should be clearly detailed to allow reuse of the Evaluation report for composition (Article 54.1.g).
- There should be a clear indication of what is the minimum information that needs to be publicly available to be supplied to the Conformity Assessment Bodies evaluating the composite product (Article 54.1.h).
- For composite certification and product, there should be composite maintenance procedures in place, including vulnerability management or vulnerability assessment procedures based on the cases and assurance levels. The rules for monitoring compliance should extend to the composite product for continued compliance with specific

cybersecurity requirements. (Article 54.1.j and Article 54.1.m).This is a complex topic and should be further discussed, including aspects linked to the market surveillance of components, dependencies, for composite products.

4 Product security certification

4.1 Certification overview

A certification scheme as defined in the EU Cybersecurity Act provides a framework within which a sound certification ecosystem can be organized. A European certification scheme is made of security requirements, a corresponding evaluation methodology and governance rules. The Cybersecurity Act suggests considering and referring to two main sources:

- European, international and industry standards that define evaluation methodologies for a given vertical or context.
- 'Security Profiles' that could be defined within a scheme and/or standard, and define precise requirements tailored for a given use case, product category, or vertical.

The EU Cybersecurity Act requires a scheme to include information about mutual recognition with other schemes, but that requirement does not address a definition of how the scheme may allow the reuse of evidence coming from other schemes, and how recognition is implemented beyond certificate-level recognition.

The objective of security certification is to demonstrate that a product complies to the security it claims. There are many ways to perform such a certification, but the information on which it is based always comprises the same elements:

- a security problem, with assets, threats, and mitigation measures as well as security objectives;
- a list of security functions, which implement the mitigation measures defined above;
- a set of guidance documentation describing how the product should be initialized, configured and integrated for its security functions to work properly;
- and a set of assurance measures, that have been used to verify that the implementation of these security functions effectively mitigate the threats of the product's security problem, when the component is used according to the provided guidance.

This information is sufficient for a security expert to evaluate the security of the product in the context of a framework. The framework will ensure that the assessments are based on a set of shared procedures, also known as an evaluation methodology, a first step for enabling comparability of the results of security evaluation. An evaluation methodology is part of a certification scheme and helps defining the steps, i.e. *what*, and the assessment techniques, i.e. *how*, that an expert needs to learn and follow to perform the evaluation in accordance to a certification scheme.

4.2 Need for Certification scheme composition

Until recently, security certification applied to a limited type of processes and products, that in most cases were designed and manufactured by the same organisation. Schemes have been defined for each product or process category, which often became more and more complex over time. For instance, a complete device can be characterised by software and hardware, so the evaluation

could be performed by different stakeholders mainly because those products could have been manufactured by different entities, each one specialized on a particular component of the product. The complexity could grow further as the software itself could be separated into generic platforms and vertical applications.

Similar splits now appear in many fields, as complexity increases. Cloud-based systems, IoT deployments in factories or in cities, and even cars, are now so complex that a global certification can only be achieved by assembling certified components. Composition is the generic name for this assembly process.

Composition applied to certifications naturally springs to mind when building a product from previously certified components. In such case, every certified component brings with it the results of its certification, together with the information related to its intended use, creating a base for composition, highlighting the critical parts of the component that require dedicated attention and re-testing when integrated in the final product.

When a product is built by assembling components, the objective is to reuse as much as possible the evidence that come with the certified component during the evaluation of the composed product. However, some integration steps will require re-testing of the component when the set of assumptions on the environment or intended use changes. For instance, if hardware IP is integrated into a new chipset, some physical properties may be modified, so it is necessary to repeat some of the tests, to ensure that the conclusion of the component evaluation is still valid.

Even in the simplest case where a product is built on top of a single component, maximising reuse is not easy: specific tasks must be completed to link the security problem, security functions, and assurance measures of the component to the product's definition and to ensure that the component's guidance is followed in the development of the product.

With today's complex products and components, composition must be envisaged, and in most cases, several layers of composition will be required. In order to simplify the work of product developers, it becomes necessary to establish links between the various cybersecurity certification schemes, evaluation standards, and industry-specific requirements. Such links are prerequisites to make the certification workload acceptable for complex products.

4.3 Out of Scope

The following issues, or limits of the composition, are outside of scope of this document although they could provide the focus of future work:

- The maintenance process and the management of the certificates' validity are scheme dependent, as such its implementation is out of the scope of this document, which has the intent to be standard and certification scheme agnostic. Related questions will be addressed by each EU scheme or at the level of the EU certification framework.
- Therefore, composition using certified components outside the validity period of their certificates is not considered in this document.
- Composition with certified components for which vulnerabilities have been discovered since their certification. This scenario will require a specific process that may be defined by the scheme for certificate maintenance. The voluntary characteristic of the EU certification

implies that the re-certification of the ICT product, impacted by a new vulnerability in the validity period of the certificate, relies on the decision of the owner of the product. For example, the way to address this topic is initially tackled by the first draft of the EUCC scheme [8]. The use of that product (without re-certification) for a composite certification will require a proactive impact analysis of the changes/updates and contractual relationship between the owner of the product and the composite manufacturer.

- The detailed definition of the relationships and rules for sharing evaluation outputs between evaluation labs (including liability issues) is outside the scope of this document. Possible frameworks may be proposed by each EU scheme that allows and facilitates the composition.

5 Product certification composition considerations

Composition is about reusing the evidence and results provided in support to a security certification of a product (the component[1]) in one process in the certification of another product, based on a different process. There are different ways to use composition, though, depending on a variety of factors:

- How composition is performed, i.e. how the component is used in the composite product.
- How the schemes used for the component and the composite product are related.
- How the manufacturer of the composite product wants to reuse the evidence from the component's certification.

There are nevertheless a few common rules about composition that apply in most, if not all, cases:

- The composite product integrating the certified component should satisfy the assumptions on the intended use and the environment from the certification of the component.
- The approach taken in this document will start with the risk assessment / threat map of the final product and the correlation of its final product security profile vs the security profile (security functionalities) of its components.

The goal is to have a clear understanding of how deeply the final product relies directly on the certified security profile implemented in the components and therefore identify the security functionalities that were already certified, needing mainly a detailed verification of its correct usage.

As the security of the whole product depends on the security of its components and the security of the interactions between them, it is necessary to clearly identify the different interactions between the product and the components and between the different components used within the product itself.

An exhaustive identification of such interactions is crucial to ensure that any vulnerability, weakness or security flaw is discovered. This also leads to the challenge of analysing of potential cascading effects, i.e. how risks, vulnerabilities and security flaws will propagate and impact other components or the products when the composition is achieved. The risks identified within the components can be more or less critical depending on the propagation and effect of the vulnerability over the composed product.

A product composition approach can contribute to greatly reduced costs and time spent when a component is used in different products, thus, allowing the reuse of evidence from the component during the evaluation and certification process of the product. However, reusing the evidence as much as possible is not always an easy task. A careful analysis is necessary to determine what can be reused and what should be discarded, repeated or modified. As reviewed before, the

[1] In this document, a component is defined as a product used in the final product, and it can be both hardware and/or software.

assurance level at which a component is evaluated influences the reuse level that can be achieved. **If a component is not evaluated at least at the same assurance level of the final composite product, then, significant additional work might be needed to assess the final composite product.**

This section will discuss the procedures and the related challenges that needs to be addressed to reuse the evidence and enable composition.

A composition approach could be built in the following different ways:

A Bottom-up Approach

As discussed earlier, this is typically driven by some generic requirements defined on the underlying components (Platform) level independently from how they would be applied on the top components (Application) level. In this approach, security features are set up like building blocks allowing the top component layer to pick the platform that covers the final application security goals.

- Advantages. With this approach, the underlying components standalone certification is straightforward and could be done once for all verticals. Guidance is provided to the top component layer allowing developers to minimize the risks of a composite evaluation failure.
- Drawbacks. Such approach is generally not adapted to all intended uses and might be exceeding or not meeting the security goals of the final composite product certification. For instance, the Application might require additional security features not provided by the Platform. In addition, many assumptions are generally made to reduce the threat attack surface, thus making it difficult for the top component to customise them to properly fulfil the intended use. Finally, the risk-owner is generally not included in such an approach making it difficult to balance between the applicable security requirements and the accepted risk.

A Top-Down Approach

This approach consists of a composition that is made from the ICT product's end usage perspectives. Indeed, the intended use of the final ICT product in its operational environment governs the requirements on how this product should protect itself against cyber-attacks. A risk-based approach is therefore required to identify the risks at the top level of composition (e.g. the application level) at a first stage before setting the security requirements for having specific security features provided by the bottom components (e.g. the platform level).

- Advantages: This approach allows a more objective and cost-efficient composition meeting the business line needs. Indeed, one ICT product could end up operating in different operational environments and could have different users with disparate identified risks which require different types of security features certified at a more or less security assurance level. As an example, a connected camera installed at home might require less security features than when it is set up outdoor to observe an ATM. By opting for a Top-Down composition approach the application vendor can have a more granular choice of using a certified platform.
- Drawbacks: The risk-based approach must be based on a standardised risk assessment methodology to insure harmonisation of the requirements.

Bottom-up and Top-down approaches complementary

Those two approaches presented above can in fact be practically combined to fit the market security needs.

Indeed, the Top-down approach is typically used by the Original Equipment Manufacturer (OEM) or system providers, that perform the risk-assessment and select the optimised cost-efficient solution.

Whereas, the Bottom-up approach is best suited for a "general purpose", vertical agnostic security offer providers. It is typically used by chip or platform developers, providing general purpose ICs/microcontrollers with embedded software implementing security functions with scalable security robustness (e.g. lowest cost, providing security functions assessed with 'basic' assurance; security functions implementation resistant against cyber attacks carried out by actors with limited skills and resources, with 'substantial' assurance; security functions in dedicated security ICs, resistant to highest attack by actors with significant resources and certified with 'high' assurance).

Practically, if we consider the intended usage of an ICT product, the risk mitigation priorities will vary accordingly. For instance, if we place a connected camera at home it should require less security countermeasures (e.g. user privacy enforced by strong authentication, encryption) than when it is set up outdoor observing an ATM (e.g. camera integrity and keys' confidentiality enforced by a strong physical shield and a secure element). In such case, the camera vendor will use a Top-down composition approach to choose the appropriate component/platform, that has been certified Bottom-up.

5.1 Composition with single and multiple schemes

The relationship between the scheme used to certify a component and the scheme used to certify the composite product, that includes the component, is essential since one of the main issues for composition is the achieved assurance level and the mapping between the evidence (that depends on the assurance level) required for the composite product and the evidence provided and assessed for the component.

Composition within a single scheme

Composition within a scheme takes as its reference the security functional and assurance requirements meeting a security assurance level defined in the context of a scheme. Such a scheme could be aiming to cover a large domain of applicable items, for example a whole vertical (e.g. consumer IoT products). The way the composition evaluation runs in that case is by building on top of certified evidence some remaining evidence that all the security functional and assurance requirements are satisfied. This approach requires no mapping or translation of the elements that the evaluator reuses from the component certification. It requires nevertheless a proof of adherence or compatibility of the security features that are reused on the composite product level.

As an example, let's take the case of a consumer IoT product, e.g. a smart camera. The secure processor of the camera will be in charge of establishing the root of trust in terms of software/firmware authentication, as well as providing several crucial security functionalities, such as a crypto engine or a random number generator.

Once the processor is evaluated and certified, the evaluation results can be directly considered in other product evaluations in which the same processor (with the same version) is used. The processor becomes therefore a (certified) building block.

On top of the processor will be the firmware of the product. This firmware will rely on the (certified) security features offered by the processor and build on top of that product specific features (such as authentication, authorization, session management, etc.).

The secure processor with the firmware could be certified in a composition under the scheme while taking into account that its security features will be reused by another component in a composite certification.

Finally, the software application running on top of the firmware makes use of the security features provided by the firmware and is in charge of using them in a correct and secure way

In a case where a smart camera application developer chose to run a composite certification upon the certified secure processor, the choice of a single ("same") scheme will allow her/him to rely on the same type of evaluation methodology while proving that the application relies on the root of trust functionality to guarantee the application authenticity. The evaluator's activity will be more focused on other security functionalities specific to the application to complete the evaluation report at the required assurance level. Of course, an important aspect is that the interconnection of the building blocks is assessed separately, to ensure that no vulnerabilities are introduced by the composition.

Composition within a single scheme is made easier due to consistency in those policies, procedures and the used evaluation methodologies applied in the certification scheme.

Composition with multiple schemes

Cross scheme composition principles should be the same, with the difference that instead of adapting the requirements of a single scheme to fit all the building blocks, different schemes are accepted for validating the security of the individual evaluation elements.

By relying on the previous example, the processor could be evaluated and certified based on a specific evaluation scheme (for example EUCC), the firmware running on top of it under a different scheme, and finally the applications under a different one. Attention needs to be paid again to the secure integration of these building blocks, an operation which is under the control of the final product manufacturer. At the same time, other process and procedure specific schemes could be considered for covering, as an example, the secure manufacturing process or the process of deploying firmware updates after the product is released.

5.2 Composite product

There are different ways to build a composite product from certified component, which influence how the component's certification may be leveraged in the certification of a composite product.

A component may be an independent product.

In this case, the component addresses a specific security problem, which is relevant for the composite product. The typical characteristics of an independent product are encapsulation (it can easily be separated from the other components of the composite product), and limited accessibility (it can only be accessed using a dedicated API or physical interface, on which it applies access control measures). In such cases, the certification of the independent product may be accepted as a whole, with limited requirements to reassess the evidence.

In addition, an independent security component may be entirely responsible for some of the device's assets, ensuring the protection of a subset of device's assets or providing the security functionalities that mitigate the risk identified on a subset of device's assets, typically cryptographic keys and credentials. In this case, the component may be certified with higher assurance requirements than the composite product, provided that it is possible to identify a consistent subset of the composite product's security problem. As examples we can highlight:

- **An independent component is a secure element with a specific function**, such as the SIM card used in mobile phones. The SIM card is part of the product, but its security is evaluated and certified separately from the phone's. In addition, it is likely that a SIM card be evaluated with an assurance level that is greater than the phone's, because it protects assets that are essential for the network operator.
- **Car-to-Car Communications Consortium for the certification of V2X vehicles**. The security problem has been split between a Hardware Security Module (HSM) and a complete module that includes the HSM, and the assurance requirements are higher for the HSM.
- **Smart metering.** A smart meter may embed a secure element to store the sensitive assets (and to perform sensitive security operation). The secure element is evaluated at a high level using a specific scheme such as the SOGIS CC and the meter could be certified at a low level using a lightweight scheme, e.g. CSPN [9], BSZ [10], or CPA [11], or even a specific scheme for smart energy.

A component may also be tightly integrated in a composite product.

This is the most common case, when a component is used to implement some of the security functions from a larger product. When this is the case, it is often difficult to determine a precise subset of the product's security problem that is addressed specifically by the component. Instead, the component contributes to the implementation of some security functions.

Depending on the nature of the component and on its integration, the reuse of evidence may be limited based on the scheme and composition types, in particular when it contributes to a large or generic objective.

Typical examples of tight integration are cryptographic libraries. A software library runs on a composite product's chip and operating system, integrated with specific software. In such a context, it is essential to verify that the security claims from the component's certification remain true. In some cases, for instance when a composite product uses the same hardware and operating system on which the library component was evaluated, significant reuse may be possible. On the opposite, when the operating conditions are very different, it is likely that most of the evidence will have to be at least partly verified. Another example is the mobile device integrating a trusted execution environment (trusted OS) for which the Root of Trust (RoT) and secure boot are implemented by

the underlying SOC. The mobile device, the composite product, could be certified at a lower level that its components, the trusted OS and the SOC.

5.3Composite assurance level

The level of assurance of a composite product made of certified components depends on the scenarios mentioned in the previous section, i.e. composite product in the same scheme or cross scheme composite product.

Product's Level - Single Scheme (Product Composition)

In the context of product composition in the same scheme, based on the well-known concept that the security level of a set of components is equal to the weakest security level, it seems quite straightforward that the assurance level of a composite product could not be higher than the lowest assurance level of the components. **In case of reuse of certification results and assurance evidence, the assurance gained on the composite product will rely on the component assurance level that is reused as it could not be modified.**

For example, using the three assurance levels of the Cybersecurity Act (see Section 3.2), a composite product made of certified components at *substantial* level will achieve only the substantial level, without retesting. As the component's security functionalities have been evaluated at a level intended to minimise the risks from attackers with limited skills and resources, the composite product could not be evaluated with respect to high-skilled attackers without re-evaluation of all the functionalities of the composite product. In the context of Common Criteria, examples are the secure element with the hardware certified at a higher level that the composite product made of applications, software platform and the hardware chip. Another view uses the depth and rigour criteria of the evaluation; the assurance level of the composite product will correspond to the level of rigour and depth used to evaluate the components as the evaluator has no possibility to re-evaluate the components.

A sub case of this approach uses the multi-assurance feature when allowed by the scheme: a level of security assurance could be defined at the level of a specific security functionality in a product. The Security Target may identify a subset of Security Functional requirements requiring higher assurance than the one required by the whole product. Such composition could apply a multi-assurance (or level of security assurance), "Basic" security assurance for the product, with "High" security assurance augmentation for specific security functionalities. For instance, an application could define security requirements enforcing protection of critical assets such as cryptographic keys or credentials from physical tampering/attacks. This requires the usage of a tamper resistant component like a secure element to meet such requirement. At the same time, other security requirements are defined for the same product requiring lower security assurance, and, therefore, lower means of protection, e.g. for non-sensitive user data. This approach is heavily used by the Common criteria scheme using "augmentation".

Product's Level – Mixed Schemes (Scheme Composition)

In case of schemes composition, i.e. components are certified in different schemes (and possibly at different levels), the approach is the same as above if all the schemes use the three levels defined by the Cybersecurity Act. But the "nature" of the composite product is of relevance. If the

composite product is made of components that cooperate, e.g. a system, the assurance level will rely on the dependencies between the components and deciding about the resulting assurance level is not straightforward.

The interesting point is the meaning of the assurance level of a composite product that is part of "*the certificate meaning improvement*" objective of the EU certification framework. For example, a product certified at a basic level that integrates a component (a crypto library) certified at high level, what is the meaning of this "basic" assurance level for the customer/end user? Another example is a mobile device integrating a Secure Element (SE) or a Trusted Execution Environment (TEE) certified at a "high" level that gets a certificate "basic", what is the meaning to the end user, e.g. "basic" certificate although the most sensitive component TEE and secure element have been certified at "High"?

5.4 Considerations on certification evidence reuse

As we have seen above, composition is about reuse of (assurance) evidence, usually to reduce the amount of work required for the certification of a composite product. In some cases, certification costs may be very high, especially when regulators or market conditions include high-level assurance requirements. High levels of assurance imply a deep vulnerability analysis and penetration testing that require high skills, time and tools & equipment.

In such a case, it can be essential for the viability of a use case to ensure that the evidence from a component be reused with minimal verification by the composite product's evaluator. For instance, when resistance to hardware attacks is required, the certification of chipsets can be very expensive, as it includes complex attacks with sophisticated equipment. It is then essential to ensure that these attacks will not need to be repeated when application software is added to the chipset. Another high effort consuming work is the testing and certification of random number generators. Re-use of results among identical platforms is essential.

Other activities such as site audit may be expensive, especially for composite product made of several components. The site audit results made for each component should be reused for the composite product certification. Obviously, the sharing of the site audit results should be only based on the certificate of the components and not on the report contents that is generally a sensitive information.

5.5 Modular approach

In order to improve the security evaluation process, we've seen some use of incremental and modular evaluation methods based on a modular approach of defining security requirements. Those approaches are expected to minimize as much as possible the tough task of security re-evaluation when addressing new composite products including some variants in their functionality.

This modular approach optimises the composition constraints platform/applications by minimising the adaptation charges of applications. That could be translated in the creation of simple and systematic approaches that identify and validate those adaptations.

How does it work?

The modular approach considers that if we define a Baseline of security requirements (Base-SR) taking into account a baseline threat model which is common to a type of products, and later on we define an implementation-independent set of complementary security requirements (Module-SR) to the Base-SR, the vendor would be able to choose any configuration of Base-SR and Module-SRs to evaluate its final products against. This allows the evaluator to focus his effort on the identified delta.

Let's consider we have a certified OS that is intended to be bundled with different standalone third-party healthcare applications. The security needs may vary from a market to another, for instance when it comes to the cryptographic primitives to draw from. Therefore, if these security needs are already addressed in different Module-SRs, the vendor would be able to create a configuration and approach an evaluator to conduct a quick composite evaluation without having to completely re-define the security problem definition.

Limitations

We note that there could be some limitations to this approach in case the Base-SR requires modification to adapt to a security functionality change at the OS level for instance, this will require processing a delta evaluation of an already certified configuration.

6 Product certification composition guidelines

The guidelines for certification composition are based on the following assumptions:

1. We are in the context of European Cybersecurity certification framework and certification schemes are EU schemes compliant to the Cybersecurity Act (see Section 3 for the specific requirements), e.g.*:*
   a. The content of a certificate such as validity period;
   b. Each scheme may include one or more assurance (of the three) levels.
2. All certificates of the certified components are valid at the time of composition.
3. The (cyber) security risk analysis used to derive the security profile is the same across the schemes:
   a. A set of assets is identified along with a set of threats on those assets;
   b. A set of security objectives and/or requirements (e.g. confidentiality) to counter those threats;
   c. A set of security functionalities/features/controls (e.g. encryption) that the ICT product implements to fulfil/answer the security requirements.
4. The EU cybersecurity certification schemes considered allow for certification composition. This statement implies that the scheme allows/implements mechanisms and processes for the sharing of certification evidences. The minimum set of evidence will be detailed later in this document.
   a. Several important aspects need to be taken into consideration when defining a scheme that allows for composition. These aspects can contribute to ensure the scalability of the scheme, maintainability of the issued certificates, as well as the smooth integration between certificates and results of various components in the composed evaluation target.
5. Each EU cybersecurity certification scheme considered for composition defines, as a minimum, the following outputs from a certification:
   a. A certificate identifying the version of the product/component that has been certified, and the level of assurance.
   b. A security target (may include a public and confidential part), that includes assumptions on the environment of the product/component.
   c. Guidance for end user/integrator. This guidance provides information for secure installation, configuration and use of the product/component.
   d. An Evaluation report, that includes a confidential part and a public part to be used for composition (an example is JIL *ETR for composition).*
6. There are other aspects that need to be considered and that will influence the composition
   a. The certification scheme (see Section 5.1)
      i. The composition is done using the same scheme for composite product than the one used for the certified components or
      ii. the components have been certified in a different scheme than the one to be used for the composition.
   b. The relationship between the provider of the component and the final product

   i. The manufacturer/developer building the composite product and applying for certification by composition is the owner/developer/manufacturer of the components already certified to be used for composition.
   ii. The manufacturer/developer building the composite product and applying for certification by composition will use certified components from a supplier/another manufacturer/developer.

c. Standalone components or component implementing a specific functionality (see Section 5.2).

7. The following scenarios are out of scope (see Section 4.3) and may be investigated in a second step:

   a. The certificates of certified components to be used are out of date.
   b. The certificates are still valid, but a major new vulnerability (or vulnerabilities) have been discovered since the issuing date of the certificate.

6.1 Risk analysis and secure design

The building of a composite product follows the secure design architecture. The security target is built following a risk analysis, starting from the assets of the product to be protected down to the secure functionalities/controls implemented for that protection (note that assets are not only data such as credentials but may include secure services). Therefore, **the security target of the composite product will list the assets and the security functionalities/controls required for their protection**. Some security functionalities may be provided by the certified components.

This simple methodology could be more sophisticated in case the required security functionality is implemented by several certified components, or the assets of the composite product are the result of an aggregation of the assets of the components, etc.

Moreover, the risk analysis uses the threat model for the composite that may be different from the threat models of the components. For example, a certified component that considered an attack model without physical access is used for a composite product considering a hostile environment with physical access by the attacker. This scenario will be forbidden by the assurance level composition, i.e. targeting a “high” level with certified component at “substantial”.

6.2 Security target

One of the most important parts of content of a security target regarding the composition is **the set of assumptions on the environment in which the certified product will be used or will operate**. The environment has been used in the risk analysis to build the security target.

Generally, some assumptions will be fulfilled by organisation measures, such as “*the administrator is a trusty actor that performs correctly his role*”, or “*it is assumed that the product will be installed and configured according to the user guidance*” (see below Section 6.3), other by technical measures “*it is assumed that the component will be integrated on a secure hardware*”, “*the random number should be provided by a good generator providing sufficient entropy*”.

Such strong technical measures are security objectives/requirements, and the composite product should provide security functionalities/controls/features that fulfil these requirements and assumptions. The assessment is performed by the evaluator during the “composite” evaluation.

6.3User guidance

The user guidance is one of the outputs of the certification that details the condition for a secure use of the certified component. The term “user” concerns all types of users, e.g. the administrator for the final product, the developers that will integrate the component developing another layer, or any role that will interact with the product.

Therefore, **the guidance should provide information about the acceptance, the secure installation, configuration and maintenance of the product in order to operate securely**, for example the length of the seed value that should be provided by the user for the secure installation or how to check the version or the integrity of an embedded software. Note that in lightweight certification schemes, that minimise the documents from the developer, this is the only piece of evidence required with the security target of the product.

Therefore, for the composition, the evaluator will check that the developer of the composite product respects the user guidance during the design or reports some measures in the user guidance of the composite product. As an example, in case the user guidance of the certified component requires a secure operation environment protected from physical access and the composite did not implement protection against physical attacks, this measure will be reported in the composite use guidance.

6.4 Vulnerability analysis

The vulnerability analysis performed on the composite product will depend on the targeted assurance level. As described in Section 5.3, the composite product could not target an assurance level higher than the lowest assurance level of the components (in the scenario 6.b.i with full re-use and without re-certification).

The vulnerability analysis and the corresponding (penetration) tests are performed by the Conformity Assessment Body (CAB) using all the information collected about the composite product and its (design) documentation. Therefore, without access to the certified component and its design documentation, the CAB will perform the vulnerability analysis using the shared component evaluation report (that may mention the residual risks), the composite security target and the composite user guidance.

6.5 Development processes

The composite evaluation will necessarily rely on the component evaluation report for the development processes and site audits, if required by the scheme and the assurance level. The component evaluation report explicates what are the development and production sites that have been audited; this information should be included in the shared evaluation report. It might not

be possible, and probably not adding additional elements for the evaluation, to envisage for a composite product made of several certified components the audit of all the sites by the CAB. This is not only related to the cost but also to the capabilities and expertise of the CABs.

For the composite product, it is mainly the integration processes of the certified components, that should follow the user guidance, that need to be audited. For example, a smart meter will embed a tamper resistant secure module, for the secure storage of the keys. The secure module has been certified at “high” assurance level and the development and production processes have been audited. The smart meter is to be certified as a composite product against a specific scheme for industrial IoT. Only the integration process manufacturing has to be audited by the CAB, that will check that the security measures inside the user guidance of the secure module has been followed.

6.6 Assurance level for the composite product

As described above, the assurance levels in the EU cybersecurity certification framework are defined according to the evaluation methodology applied on the ICT product with respect to the risks that are considered from its intended usage. The evaluation methodology could be more or less rigorous and providing more or less in-depth assessment. It also covers different levels of resistance against attacks qualifying the ICT product’s level of robustness against attackers with different skills and resources. The highest assurance level could correspond to products that resist against a high skilled attacker with highly advanced means, and where highly rigorous and in-depth assessment methodology has been conducted by the evaluation facility.

The correctness or conformity of the security functionalities is a criterion that will be defined at the level of the scheme. Therefore, **combining certified components to form a composite product will also depend on the assurance criteria on the design and evaluation methodology for the correctness of that design.** This will rely on the harmonised definition of the levels for all the schemes allowing composition. For instance, the substantial level should be comparable to the substantial level of other schemes in term of requirements and efforts from the developer and in term of rigor and effort conducted by the CAB. This must cover a harmonised robustness testing methodology defined by technical domains (e.g. Smart Cards and similar devices, Security Boxes, etc.)

6.7 Basic elements needed for composition from previous security assessment

Evidence to enable composition

For composition to happen, a risk assessment needs to be executed focusing on the correct usage of the components (intended use and scope) for the definition of the threat model and security requirements. The following table focuses on the integration usage and the tested Security Target to identify the residual risk and what needs to be tested to attain the desired assurance level.

It is worth noticing that **the intended use of the integrated components should be part of the definition of the risk and how the risk is handled by the component**. This mapping needs to be done.

In the case of residual risk, additional evaluation and tests need to be covered at the application layer.

Targeted assurance level	***Component Certification Elements that might be necessary for Assessment***
BASIC	Certification: [a] Composite security Target (this includes security requirements and security functionalities) [b] End-user guidance and recommendations o Integration guideline including assumptions about the environment & configuration of the security functions [c] Composite Maintenance procedures: o Vulnerability management procedure o Patch management and end of life procedure
SUBSTANTIAL	Elements required in the assurance level BASIC + [a] Composite Development, Delivery procedures: o Configuration management o Vulnerability handlings plan [b] Composite Functional Testing [c] Composite Vulnerability Assessment [d] Composite Design Compliance: o Interfaces description o Global product architecture
HIGH	Elements required in the assurance level SUBSTANTIAL + [a] a more detailed design documents and anything required for the vulnerability assessment

6.8Generic composition model

A Generic composition model could be initiated at a Security Profile level which sets the security requirements against which an ICT product must be evaluated. Indeed, all the parts of such document as described in Figure 1 below must be ready to accommodate for a composite evaluation on the Security Target level for instance.

This effort starts by defining a Target of Evaluation (TOE) scope which is composed in layers. For a visual example of the use case, the reader can refer later to the case study in Section 7 (Figure 4).

These layers could be developed potentially by different vendors and brought together in a final product. To make this Security Profile ready for a composition by design thus guaranteeing a consistent and exhaustive evaluation of the composite TOE, the guidance below is generally followed:

- Assets must be defined in a generic way on the underlying layers of the composite TOE in order to accommodate for specific assets relevant to the upper layers (e.g. application layer). These are commonly separated in User Assets (e.g. data created and managed by the user) and in Security Functionality Assets (e.g. cryptographic keys created to be used by cryptographic operations inside the TOE) and their protection properties (e.g. confidentiality, etc.) must be defined to link them easily to the threat model.
- The Assumptions and the Security Organisational Policies that are considered in the threat model must be clear and demonstrable allowing the composite TOE to modify or add according to the threat model considered by the final application.
- The Threats and Security Objectives must be defined clearly based on a *generic risk analysis* and they must be mapped to impacted assets. The goal is to identify a common baseline of threats relevant to the different final application use cases. This approach pushes security requirements to the underlying layers to implement features mitigating these threats when possible. Note that it is very important to identify the side effects that the composite TOE may have on the Security Objectives. Usually, those side effects are unknown to the evaluator of the lower layer (e.g. HW) and are not identified at the Security Profile level.

  For example, Meltdown, Spectre or Foreshadow vulnerabilities or side effects have been imagined because they don't contradict the HW specification used by the SW developer so for the HW vendor these are not a security problem. So, the Security Problem tends not to be updated on the composite TOE (SW on HW).
- Security Requirements must be then identified and mapped to the potential functionality that is provided by each layer of the composite TOE. In addition, these should be re-mapped to the Security Objectives in order to guarantee that the security properties (e.g. Confidentiality, Integrity and Availability – CIA) remain satisfied.
- Security Assurance Activities – actions that should be conducted by the vendor and the evaluator (e.g. provide design evidence, test security functionality, conduct vulnerability analysis, etc.) of the composite evaluation must represent a subset of the security assurance activities of the underlying layer.
- Statement of Compatibility that should identify under which conditions the upper layers can trust in and rely on the certified lower layer security functionality without re-evaluating them.

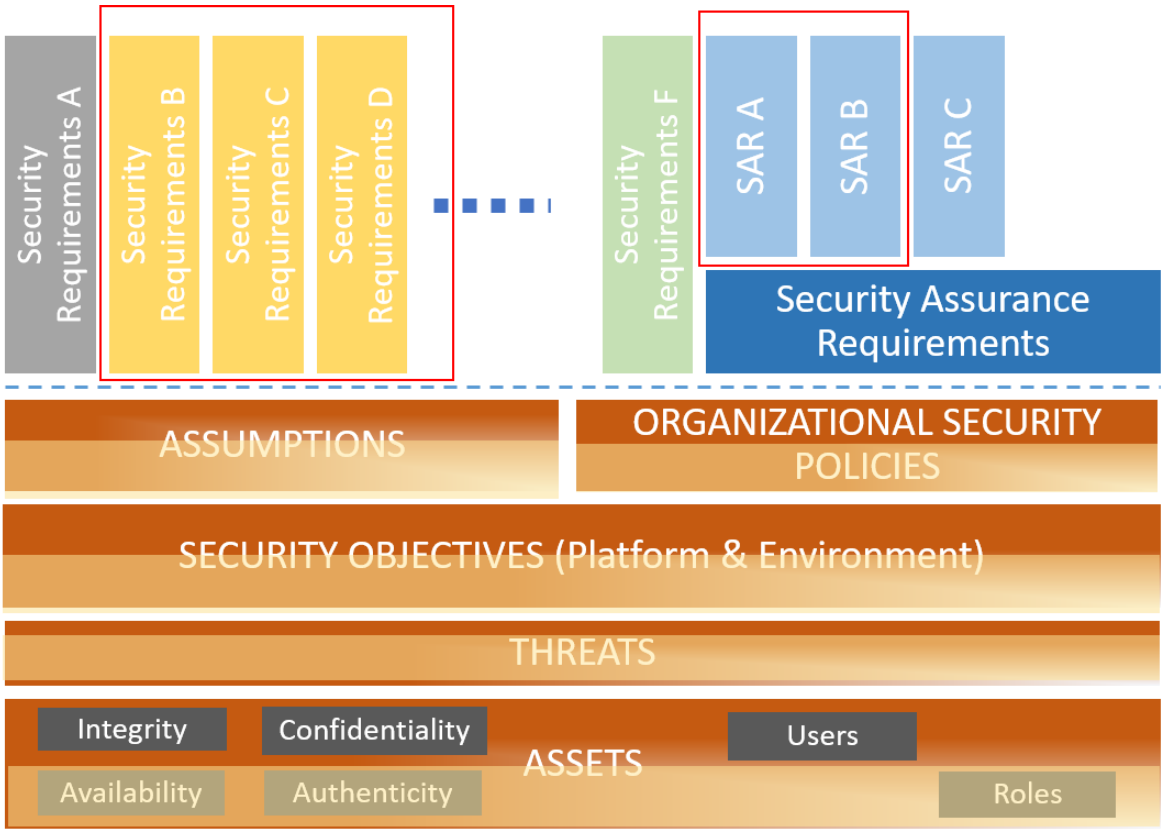

Figure 1 - Composite Security Requirements

7 Reference study case

7.1 IoT Connected product

The reference use case selected for this report will be based on the ISO/IEC 30141 [12] product reference and this will remain the context while the product IoT device will be explored.

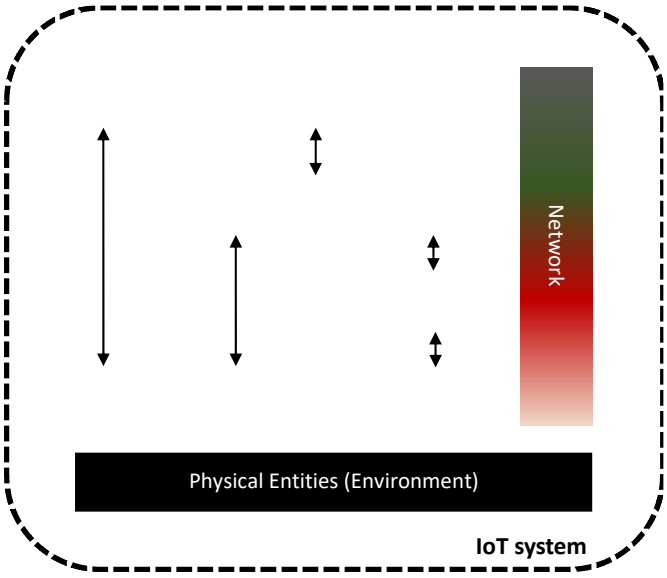

Figure 2 - An example of IoT system

The document will mainly focus on the device design and manufacture phase, see Figure 3, leaving the operational and ecosystem phases for later. It will narrow its analysis to the blue dashed box on the figure below. The definition of the connected product is important as this study will not address the "system" aspects where the integration, testing, commissioning and maintenance process are critical and must be considered in the analysis.

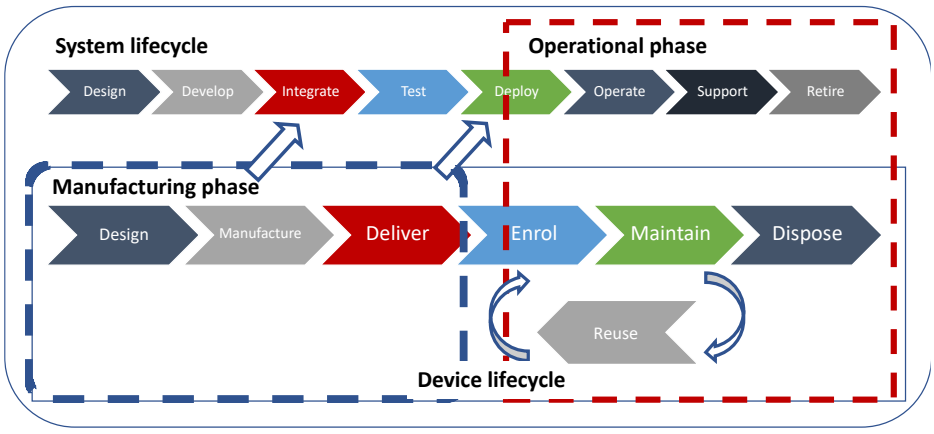

Figure 3 - Device lifecycle from birth to death: manufacturing and operational phase

For the product architecture, ISO/IEC 30141, Information technology – Internet of Things reference architecture (IoT RA) [12] will be referenced.

7.2 Product components definition

According to ISO/IEC 30141, an IoT Device is the technical artefact for bridging the real world of Physical Entities with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, processing, storage, communication capabilities. An IoT Device is attached to or in proximity to Physical Entity. In certain situations, IoT Devices can be structurally embedded in Physical Entities. In other situations, IoT Devices, especially Sensors, can be located away from the Physical Entities and monitor the Physical Entities from a distance.

More specifically an IoT device is composed of:

- **Hardware** including microcontrollers, microprocessors, mother board, ICs, physical ports
- **Software** including an embedded OS, its firmware, programs and applications
- **Sensors** which detect and/or measure events in its operational environment and send the information to other components
- **Actuators** which are output units that execute decisions based on previously processed information

Now let's split an IoT device into 3 layers of composability.

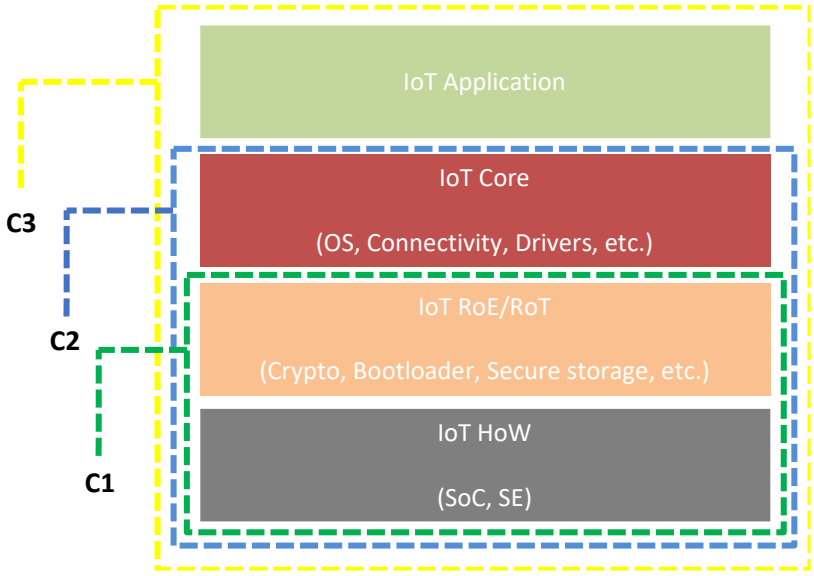

Figure 4 - Three Layers of an IoT Device

Layer C3 = IoT Application

An IoT application is an implementation of the end user functionality of an IoT Device allowing the final IoT product to fulfil its intended use in the operational environment.

At this layer, the composition certification is applied on this IoT Application assuming the IoT Core/C2 component has been already certified.

Layer C2 = IoT Core

The IoT Core main purpose is to provide trusted channel/path to external network device and allow connections to configured devices only. It includes a secure implementation of communication protocols used, a secure network connection control functionality, a secure firmware update functionality and some mechanisms to resist against logical/network-based attacks.

At this layer, the composition certification is applied on this IoT Core piece of code assuming the IoT ROE/C1 component has been already certified.

Layer C1 = IoT ROE/RoT (Restricted Operating Environment/Root of Trust) + IoT HW

The IoT ROE shall provide an environment mainly to establish the root of trust, for secure storage and usage of IoT device keys used by the IoT Core to be finally provided to the IoT Application (for its secure functionalities). It provides a level of protection against physical attacks.

The IoT HW is not restricted to a form factor, composed typically of a SoC with a Memory Control Unit (MCU), Memory, Ports and maybe an SE with no specific restrictions. The hardware may be certified in a standalone way in case it includes dedicated security services and cryptographic libraries.

At this layer, the composition certification is applied on this IoT Core piece of code assuming the IoT HW component has been already certified. For instance, the composition is possible with a security IC (Secure Element, TPM, etc.) providing enhanced security robustness for hardware attacks for security foundations.

7.3Composition in practice: product instantiation

Let's consider we have a vendor (V3) developing an IoT application based on an IoT underlying platform (IoT Core + IoT RoE / IoT HW) developed by another vendor (V2) as described in Figure 4 above. It is assumed that the IoT underlying platform has been certified by a **Conformity Assessment Body (CAB) A** at substantial level and the application has assets to be protected, i.e. a *sensitive* application. In this example, composition could be Top-down from V3 to V2, and Bottom-up from V1 to V2.

V3 would have the option to request from CAB A or any other CAB to conduct a composite certification of his final product. In order to be more accurate, V3 would have to provide a description of the product security functionality, e.g. for instance in a form of Security Target, or mapping table. This should include a **statement of compatibility** with the security functionality that are provided by the underlying platform. This could rely on **public information** made available by V2 describing the security functionality of the underlying platform.

As described in the table below, the CAB should check first that the security requirements for the composite product are fulfilled. In order to guarantee the same substantial level at the application layer, the CAB must review the security design/architecture and conduct a vulnerability analysis with the same *attack potential* level as it has been done for the underlying platform (according to the definition of the assurance levels, see Section 3.2, the underlying platform resists known attacks by attackers with limited resources and skills).

The result of the certification by composition, is described in a composite evaluation report that will complement the ones of the used components and that could support the certificate of the product that is delivered.

We assume that the scheme used for the underlying platform certification allows for composition, as described in Section 6.

Task to be performed by the CAB	Required Input for the task	Information available from the component certification (Reuse)	Rational for Reuse (reuse maximum)
Identify which security requirements of the composite product are fulfilled by the underlying platform (the certified component).	• Security Target of the composite product • List of the Security functionalities provided by the underlying platform.	• Underlying layer Security Target • (if applicable) App on Another Underlying Platform ST • The Evaluation Technical Report of the underlying platform (component) • The corresponding Certification Report • **Statement of Compatibility** based on the assumptions on the environment of the component listed in the security target, the recommendations for integration listed in the certification report, etc.	• Based on the **shared** evaluation report (for composition) of the component, it must be checked that the requirements of the underlying platform fulfil the application security requirements • Example: the application requires a secure RSA implementation, the CAB checks that the underlying platform implements/offers a RSA and vice versa: the application should fulfil any requirement about the use of the RSA implementation.
Perform a Vulnerability Analysis of the composite product to confirm the analysis (to exploit the identified vulnerability)	• The security target, providing the threat model of the composite product. • The Substantial level of assurance requires that the CAB checks the resistance of the composite product against public/known vulnerabilities. • Potential vulnerabilities	• The shared evaluation report provides information to the CAB about residual vulnerability of the certified component, mainly those that could results from the integration.	• The specific evaluation report for composition have to be used as input for the evaluation. For substantial, the underlying platform is protected against known attacks, those may be described in the shared evaluation report. Some of them may be replayed for the composition to

	coming from the analysis of the design architecture of the composite product. • Samples of the product to perform the tests. • Security architecture of the Composite Product.		check that the integration does not introduce new vulnerabilities.
Design & Conformity testing task: the CAB should check that the design of the application fulfils the "user" guidance of the certified component, i.e. the underlying platform	• The "User" guidance of the certified component. This includes recommendations for the "integration". • The conformity/design testing will depend on scheme and the assurance level in term of depth and coverage. For the substantial level, it is not yet defined.	• User guidance • Shared evaluation report of the certified component	
Composite product security guidance	• The "User" guidance of the certified component. This include recommendations for the secure "integration", that also are used to avoid introducing new vulnerabilities • Secure configuration guidance of the composite product may rely on the secure configuration	• The User guidance • The shared evaluation report of the certified component.	

	parameters of the underlying platform		
Development processes & sites	• The composite product user (customer) may have specific requirements on the "supply chain".	• The shared evaluation report describes the sites & processes audited for the certified component.	

From this example, we may notice that the composite evaluation relies mainly on the sharing of the evaluation report, including development & processes sites audit report, the integration evidence such as compatibility statement.

8 Conclusions & recommendations

The document addresses composition in an agnostic way with respect to the standards and the certification schemes with the intention to **focus on the value of the composition** for the EU Digital Single Market (DSM). The DSM will have all the imaginable diversity of products varying from consumer products, industrial products, infrastructure and many other that **will not all fit under a single scheme**. Composition can decrease time to market and certification costs while increasing assurance for multi component products.

This document highlights the importance to perform certification composition beyond the traditional single scheme and generalises the approach to cross schemes certification due to the nature of the components. In this context, a scheme adopted by the security industry may not be as relevant to the final composed product but can clearly be valuable for the security foundations of the final product, in the case of this document an IoT device. The intention is to reuse evidence of those schemes defined under the European cybersecurity certification framework explicitly allowing for composition.

With the advancement of the Cybersecurity Act in EU, and in near future with several EU schemes available to choose from, targeting horizontal, sectorial or even technological, a walkthrough guidance for composition seems to become instrumental to decrease complexity while increasing the cost effectiveness of cybersecurity and help the decision making process.

This document highlights specific aspects that should be considered by each new EU scheme allowing the composite certification, e.g. a harmonised risk-based approach to use for building the Security Profile of the composite product, a standardised format and content of the certification output evidences to be used for composition. Those aspects aim to reduce inconsistency between scheme deliverables and create an environment favourable for contribution with a facilitated re-use of certification evidence.

The composition approaches presented in this document must be tailored to the secure life-cycle development processes of ICT products or components in each industry. This provides consistency and accountability for security IPs providers.

During the development of this document, it became of utmost importance to give a special focus on the process of composition, that could be achieved either from a bottom up or a top down process or by mixing these processes, giving the developer the opportunity to choose the best choice for the design of composition and to the evaluator how to perform his task.

ECSO members have also made the effort to keep the document as generic as possible to be able not only to target composition in traditional security hardware equipment but also to propose a path suitable for software components that can in the same way benefit from such proposal.

ECSO aims for a second release of this document containing more technical details, including the operational phase (e.g. vulnerability and patch management) of the composed product, and expectations for product composition, especially when software is the focus. Other areas of interest include a practical approach for scheme composition with the first European certification schemes, e.g. cloud services and EU Common Criteria. Other aspects for further consideration are discussed in Section 4.3.

Bibliography

[1] European Parliament, Council of the European Union, *Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

[2] European Cyber Security Organisation (ECSO) WG1, "European Cyber Security Certification: Assessment Options," September 2019.

[3] ISO 19011, "Guidelines for auditing management systems," 2018.

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

[5] European Parliament, Council of the European Union, "Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC," 9 July 2008.

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

[7] ISO Guide 73, "Risk management -- Vocabulary," 2009.

[8] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Certification: EUCC Candidate Scheme v1.0," July 2020.

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

[10] BSI, "Beschleunigte Sicherheitszertifizierung (BSZ, Accelerated Security Certification)," [Online]. Available: https://www.bsi.bund.de/EN/Topics/Certification/product_certification/Accelerated_Security_Certification/Accelerated-Security-Certification_node.html.

[11] NCSC, "Commercial Product Assurance (CPA)," [Online]. Available: https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa.

[12] ISO/IEC 30141, "Internet of Things (IoT) -- Reference Architecture," 2018.

Annex 1 Article 54 of Cybersecurity Act

Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include at least the following elements:

(a) the subject matter and scope of the certification scheme, including the **type or categories** of ICT products, ICT services and ICT processes covered;

(b) a clear description of **the purpose** of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;

(c) **references** to the international, European or national **standards** applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

(d) where applicable, one or more **assurance levels**;

(e) an indication of whether **conformity self-assessment** is permitted under the scheme;

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(g) the specific **evaluation criteria and methods** to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;

(h) where applicable, the information which is necessary for certification and **which is to be supplied** or otherwise be made available to the conformity assessment bodies by an applicant;

(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate **continued compliance** with the specified cybersecurity requirements;

(k) where applicable, the conditions for **issuing, maintaining, continuing** and renewing the European cybersecurity **certificates**, as well as the conditions for extending or reducing the scope of certification;

(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;

(m) rules concerning how previously undetected cybersecurity **vulnerabilities** in ICT products, ICT services and ICT processes are to be reported and dealt with;

(n) where applicable, rules concerning the retention of records by conformity assessment bodies;

(o) the identification of national or international cybersecurity **certification schemes** covering the **same type or categories** of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;

(p) the **content** and the format of the European cybersecurity **certificates** and the EU statements of conformity to be issued;

(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;

(r) maximum **period of validity** of European cybersecurity certificates issued under the scheme;

(s) **disclosure policy** for European cybersecurity certificates issued, amended or withdrawn under the scheme;

(t) conditions for the **mutual recognition** of certification schemes with third countries;

(u) where applicable, rules concerning any **peer assessment mechanism** established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level '**high**' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

2. The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.

3. Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.

4. In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU