GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Composition and Reuse

White Paper

Introducing the Security Evaluation Standard for IoT Platforms (SESIP)

June 2021

Table of Contents

ABOUT US 3

SECTION 1: The Challenge 4

SECTION 2: Introducing the Security Evaluation Standard for IoT Platforms (SESIP) ... 6

SECTION 3: Composition and Reuse Approaches 7

3.1 Layered Composition 7

3.2 Additive Composition 8

3.2.1 Definition 8

3.2.2 Assurance Level of a Compound 9

3.2.3 Example of Additive Composition 10

3.2.4 SESIP, a Methodology Designed for Composition 11

3.3 Reintegration of a Component into Multiple Compounds 12

SECTION 4: Conclusion 14

SECTION 5: Table of Figures 15

ABOUT US

GlobalPlatform is a technical standards organization that enables the efficient launch and management of innovative, secure-by-design digital services and devices, which deliver end-to-end security, privacy, simplicity, and convenience to users. It achieves this by providing standardized technologies and certifications that empower technology and service providers to develop, certify, deploy, and manage digital services and devices in line with their business, security, regulatory, and data protection needs. Key offerings include secure component specifications; the Device Trust Architecture for accessing secure services within a device; the IoTopia Framework for secure launch and management of connected devices; and the SESIP Methodology for IoT device certification.

GlobalPlatform technologies are used in billions of smart cards, smartphones, wearables, and other connected and IoT devices to enable convenient and trusted digital services across market sectors, including healthcare, government and enterprise ID, payments, smart cities, industrial automation, smart home, telecoms, transportation, utilities, and OEMs.

GlobalPlatform standardized technologies and certifications are developed through effective industry-driven collaboration, led by multiple diverse member companies working in partnership with industry and regulatory bodies and other interested parties from around the world.

SECTION 1: THE CHALLENGE

Information and Communications Technology (ICT) products are increasingly built as composite products, assembled using a number of lower-level components. These components are also reused across a number of other composite products.

The security evaluation of composite products comprised of already evaluated elements, as well as the reuse of evaluation results across certification schemes, are therefore of critical importance. They can become major success drivers for security certifications at a cost and duration that is acceptable for ICT products that have a short lifetime or that are subsequent variations and evolutions of previously evaluated products.

For markets such as consumer and IoT where novelty, time to market, and cost are important considerations, certification often appears as an unnecessarily lengthy, costly, and laborious process. High complexity and cost of certification can lead to difficult resource allocation trade-offs by ICT product vendors. They need both to satisfy a rapidly increasing need for advanced features, and to assure strong protection of end users against cybersecurity threats.

In June 2020, the European Commission published a "food for thought" document to guide further discussions on certification. Although not an official position of the Commission, it was part of the consultation strategy for the preparation of the Union Rolling Work Programme (URWP) for European Cybersecurity Certification.

The "food for thought" document articulates a number of strategic priorities for the European Cybersecurity Certification Framework, one of them being *'Composability' of certificates,* which is described as follows:

> *'The Framework should explore the cybersecurity implications related to the composition of products to build larger system. This is to ensure that these composed systems have desired properties, with no uncontrollable or unpredictable side effects. In this respect, as products can be included in larger systems, it should be addressed how larger systems are certified, and whether the certification of parts of the system is transferable to the larger system.'*

In addition, in July 2020, following a European Commission request, a draft of a Common Criteria-based European candidate cybersecurity certification scheme (EUCC), a successor to the existing schemes operating under the SOG-IS MRA, was provided by ENISA for public consultation. The EUCC scheme refers directly to the concept of reusability of evaluation results. In particular:

> *'As part of a new certification, it shall be possible to reuse evaluation results from another ICT product certification. The applicant may therefore provide to the [Conformity Assessment Body] previous evaluation results including those related to the lifecycle of the product or the applicant's patch management approach to be re-used as evidence. The CAB shall reuse such results for its tasks when the provided evidence conforms to the requirements of such evidence required by the CAB and the authenticity of the evidence can be confirmed.'*

Composition and reuse of evaluations will be particularly beneficial to the evaluation of IoT products, with the following business and technical benefits:

1. **Reusability**. Evaluating components for composition saves both time and expense, as evaluated components can be used in multiple products.
2. **Cost reduction and time to market.** For developers who currently evaluate the components they develop, the proposed changes will have no direct impact, but the manufacturers who buy their components will benefit from decreased evaluation costs and time to market. If a product manufacturer develops and reuses its own components, evaluation costs can be shared across projects, and reduced evaluation time will decrease time to market for subsequent products.
3. **Differentiation.** For developers who do not currently evaluate the components they develop, reusable evaluations would be a differentiator that could increase sales.
4. **Security by design**. When a final product uses pre-evaluated components, the end developer offloads the security functionality to the security specialist who developed the already evaluated components. The security assurance of the final product can therefore leverage the already evaluated components.

It is imperative to encourage the expansion of security certification to a wider set of products, without compromising the quality of evaluations. Such expansion will lead to higher security assurance levels within the entire ICT ecosystem, and directly benefit end users. Composability and reuse of evaluations is an essential mechanism to achieve this. This paper presents several ways of implementing composability and is intended to stimulate discussion on these topics.

SECTION 2: INTRODUCING THE SECURITY EVALUATION STANDARD FOR IOT PLATFORMS (SESIP)

The Security Evaluation Standard for IoT Platforms (SESIP), developed by GlobalPlatform, is an evaluation methodology that favors composition. SESIP allows the evaluation of product parts individually or in composition, in such a way that the evaluation results of the individual parts remain applicable in different composed products.

In this document we use the term **element** to describe the device / product / platform / hardware IP block being evaluated. The term **component** describes an element that is intended to be further integrated into a higher-level element which is called a **compound**. The compound can reuse evaluation results from already evaluated components. A compound may itself become a component of another compound.

Several approaches are possible to facilitate the evaluation of a compound and the reuse of evaluation results of its components:

- Evaluating an element layered on top of an already evaluated element and benefiting from security services offered by the already evaluated element.
- Evaluating a compound assembling one or several components, previously evaluated or not.
- Reuse of full or partial evaluation results of a component when integrated into multiple compounds.

Combinations of those approaches can also be envisioned. These composition and reuse approaches are described in the following sections.

SECTION 3: COMPOSITION AND REUSE APPROACHES

3.1 LAYERED COMPOSITION

In a layered composition model, the compound is built by layering one element on top of another one as shown in Figure 1.

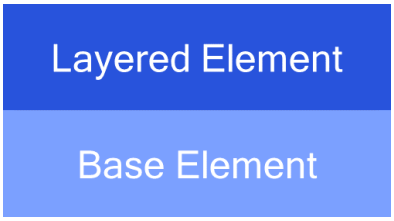

Figure 1 – Layered composition

Evaluation of the compound is achieved by evaluating the interaction between both elements and reuses the evaluation results of the base element for evaluating the layered element.

The layered composition approach has been used for many years, including for the evaluation of an application on top of an already evaluated hardware platform. In the technical domain of “Smart Cards and similar devices”, SOG-IS MRA composite evaluations, targeting highest assurance levels, are defined as a layered approach composed of a hardware platform (typically a secure integrated circuit) and embedded software layered on top of the hardware platform.

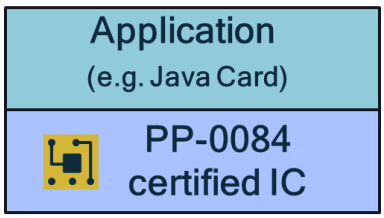

Figure 2 – Application evaluated on top of a certified Secure IC

Also, in practice, composition is very often linked with multi-assurance. Common Criteria includes ‘modular requirements construction’ with multi-assurance.

However, the Common Criteria composite and multi-assurance rules are very stringent and complex for the IoT ecosystem, especially for basic and substantial levels of assurance.

3.2 ADDITIVE COMPOSITION

3.2.1 DEFINITION

Additive composition, as defined by SESIP, is a composition by assembly approach where several evaluated components are assembled to build a new compound that will be evaluated as shown in Figure 3. Additive composition includes the traditional layered composition described previously in section 3.1.

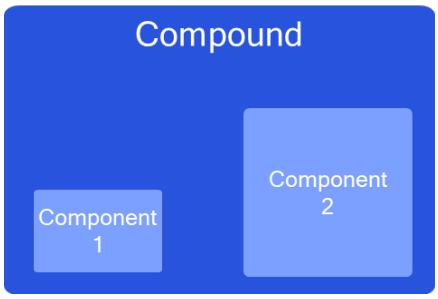

Figure 3 – Additive composition

The developer of the compound will have to demonstrate that all identified security requirements are either met directly by the compound and / or fulfilled by one of the components. The evaluation facility shall verify that:

- All security requirements are fulfilled or clearly identified in the compound.
- Either all guidance is fulfilled by the compound or its component(s), or not fulfilling some guidance does not lead to any vulnerabilities.

Composition under SESIP is designed also to verify that the objectives for the environment of the components are met for the compound.

The main advantage of this approach is that if the compound relies on component(s) for certain security services, the evaluation facility will not have to fully re-evaluate the already evaluated component(s).

Once evaluated, the compound may itself be used as a component of another compound.

3.2.2 Assurance Level of a Compound

The compound resulting from such an assembly will be evaluated at its own assurance level. Note that the assurance level of any component used for assembly does not guarantee the assurance level of the compound, but does not limit it either.

Assembly may occur between components at different assurance levels. By default, in SESIP, the compound can claim at most the lowest assurance level of the components it is assembled of. It is also possible for the compound to claim an assurance level higher than the lowest assurance level of its components. For this, during compound evaluation, the compound must provide the necessary evidence and undergo the required penetration testing to meet the targeted higher assurance level.

As an example, a communication module at SESIP Assurance Level 2 is invoked by a module at SESIP Assurance Level 3 that adds stronger security features (e.g., side-channel counter measures). As part of the compound SESIP Assurance Level 3 evaluation, the evaluation results of components will be reused as much as possible, and source code analysis and penetration testing of the compound may be necessary to establish that it does not leak sensitive information.

In addition, the compound may identify a subset of security requirements needing higher assurance than claimed by the component(s). The compound can then claim this higher assurance for these specific requirements by providing additional evidence which will have to be further examined and tested during evaluation of the compound.

3.2.3 *Example of Additive Composition*

A semiconductor hardware compound can be composed of several lower level evaluated components. For instance, a hardware block can integrate a cryptographic component and a secure processor component.

This evaluated hardware block can be further integrated into a hardware module that can also integrate an evaluated secure storage hardware component. This hardware module can itself be evaluated, leveraging the evaluations of the two components it comprises.

Finally, an IoT device can be composed of already evaluated modules or platforms, making the certification of the IoT device easier, faster, and cheaper.

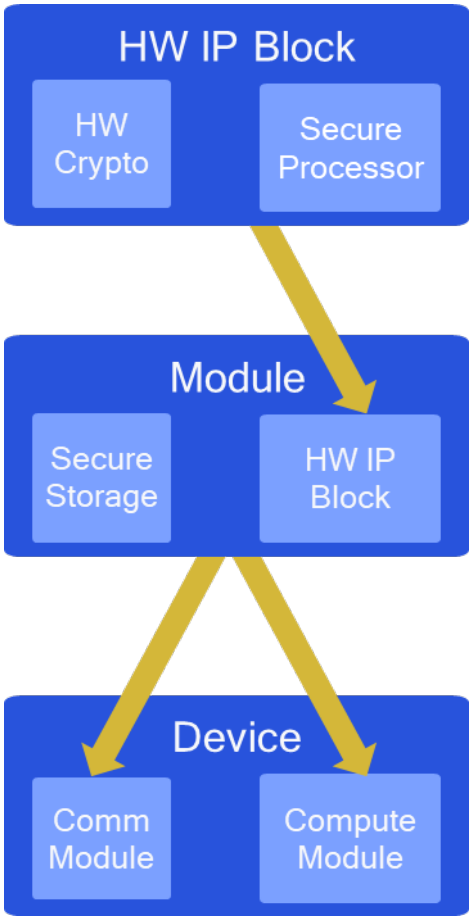

Figure 4 – Example of additive composition

In this example, all supply chain actors benefit from the additive composition approach.

3.2.4 SESIP, A METHODOLOGY DESIGNED FOR COMPOSITION

Components can be either sourced from third parties or developed internally by the compound vendor. Using SESIP as a core methodology benefits compound vendors, giving them a clear understanding of the assumptions and guidance related to the components they integrate, and enabling them to reuse evidence provided by the components' vendors during the evaluation of their compounds.

The compound guidance will identify the relationships and dependencies of the compound with, and between, its components. The evaluation process needs to accommodate this approach as, for some specific markets such as IoT, this method is essential to meet time and cost constraints.

Individual evaluation of a component must produce composition guidelines listing the rules that should be respected by any compound integrating it. These must be described as an objective for the environment and referred to specifically in the guidance. Evaluation of the compound must then assess that the guidance (including objectives for the environment, user guidance, integration guidance, etc.) associated with each component is respected. Evaluation of the compound must also assess the impact of the composition on the correct security functioning of the component(s).

Additive composition must allow evaluation of a compound using a scheme that is different from the scheme(s) used to evaluate its components. In the example presented in section 3.2.3, the hardware IP block and the module may be evaluated using SESIP while the final device may be evaluated using a scheme specific to the vertical domain of this device, such as IEC 62443-4-2 conformance certification by ISASecure.

It is therefore necessary to harmonize the concept of composition so that its usage is aligned across schemes.

The additive composition of SESIP aims to facilitate the evaluation of a compound by reusing the previous evaluations of its components. Note that SESIP specifically targets the IoT market (as the letter "I" in its acronym indicates), and defines five hierarchical levels of assurance, SESIP Assurance Level 1 (self-assessment) through to SESIP Assurance Level 5 (resistance to High Attack potential), where each SESIP level maps to the corresponding level of vulnerability analysis (AVA_VAN.1 to AVA_VAN.5 [1]).

[1] Note that SESIP4 and SESIP5 require a prior Common Criteria evaluation with corresponding AVA_VAN.4 or 5 level.

3.3 REINTEGRATION OF A COMPONENT INTO MULTIPLE COMPOUNDS

In the reintegration approach, a component that has been evaluated in Compound 1 is later integrated “as is” in Compound 2, as shown in Figure 5.

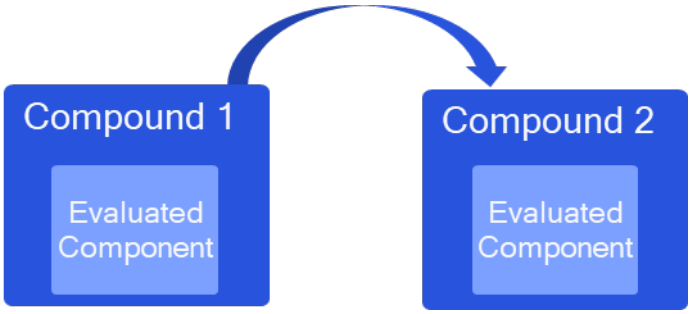

Figure 5 – Reuse of a certified component from one product into another

This new approach will be particularly suitable in support of the evaluation of components that expose a fixed set of interfaces, as it will allow for reuse of evaluation evidence. This will enable a significant reduction in the costs associated with time- and resource-consuming hardware penetration testing, required for high assurance level evaluations.

For instance, the same component can be reused in product variants spanning tiers, dedicated to specific verticals or markets (e.g., the same component can be reused across mobile, automotive, or IoT variants), dedicated to specific regions, or customized for particular customers, as shown in Figure 6.

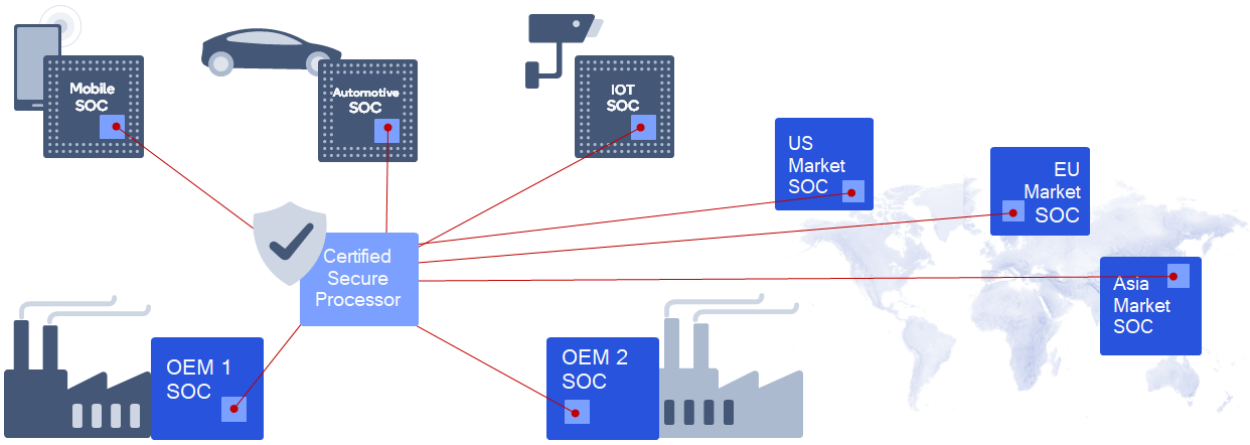

Figure 6 – Semiconductor secure processor reused across system-on-chip variants for specific markets, regions, or customers

The initial evaluation facility may identify relationships, dependencies, and expectations of the component with respect to the compound within which it is initially integrated and evaluated.

In certain cases, evidence of resistance against certain attacks can be fully ported across multiple host compounds. This is particularly true in the case of logical attacks (e.g. software attacks) as opposed to physical attacks (e.g. laser or fault injection). Such portability can be achieved by virtue of self-containment of the evaluated security functionality and the fact that the initial compound provides a proper test vehicle for a conclusive evaluation.

If full portability of evaluation is not possible due to evaluation limitations imposed by the initial compound, the evaluation facility performing the initial evaluation will identify guidance and a set of activities that need to be performed on subsequent compounds to port the evaluation results. This information will identify all the relationships and dependencies linked to the initial compound, and relevant to security evaluations, to help the evaluation facilities that evaluate subsequent compounds to be more effective. Based on this information, subsequent evaluation facilities will be able to assess whether the identified relationships or dependencies are met in subsequent compounds. If changes occurred, the evaluation facilities will have to evaluate these changes and confirm that there is no impact, or that the new integration provides equivalent or better protection measures.

SECTION 4: CONCLUSION

This paper introduced the concepts of composition and reuse, and how they can greatly reduce the cost, effort, and duration of the evaluation of ICT products. It then showed how SESIP efficiently addresses such needs, proposing a methodology that allows the reuse of evaluation results across products integrating evaluated components, and the evaluation of any type of composition of components.

GlobalPlatform anticipates that these approaches will benefit all stakeholders of the supply chain throughout the industry. GlobalPlatform is also confident that certification authorities, standards bodies, and associations will embrace the SESIP composition and reuse approaches in their current and future schemes.

GlobalPlatform welcomes collaboration from the entire ecosystem. Interested parties can download the methodology from https://globalplatform.org/sesip/ and contact GlobalPlatform at secretariat@globalplatform.org to help the organization encourage the expansion of security certification to a wider set of products, without compromising the quality of evaluations.

SECTION 5: TABLE OF FIGURES

Figure 1 – Layered composition 7

Figure 2 – Application evaluated on top of a certified Secure IC 7

Figure 3 – Additive composition 8

Figure 4 – Example of additive composition 10

Figure 5 – Reuse of a certified component from one product into another 12

Figure 6 – Semiconductor secure processor reused across system-on-chip variants for specific markets, regions, or customers 12