SLOVENSKI STANDARD
oSIST prEN 17927:2023

01-februar-2023

Standard ocenjevanja varnosti za platforme IoT (SESIP) - Učinkovita metodologija za uporabo ocene kibernetske varnosti in ponovno uporabo za povezane izdelke

Security Evaluation Standard for IoT Platforms (SESIP) - An effective methodology for applying cybersecurity assessment and re-use for connected products

Sicherheitsbewertungsstandard für IoT-Plattformen - Eine effektive Methode zur Anwendung der Cybersicherheitsbewertung und Wiederverwendung für vernetzte Produkte

Norme d'évaluation de la sécurité pour les plates-formes IoT (SESIP) - Une méthodologie efficace pour appliquer l'évaluation de la cybersécurité et la réutilisation des produits connectés

Ta slovenski standard je istoveten z: **prEN 17927**

ICS:

35.030	Informacijska varnost	IT Security
35.240.95	Spletne uporabniške rešitve	Internet applications

oSIST prEN 17927:2023 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17927

December 2022

ICS 35.030; 35.240.95

English version

Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products.

Norme d'évaluation de la sécurité pour les plates-formes IoT (SESIP) - Une méthodologie efficace pour appliquer l'évaluation de la cybersécurité et la réutilisation des produits connectés

Sicherheitsbewertungsstandard für IoT-Plattformen - Eine effektive Methode zur Anwendung der Cybersicherheitsbewertung und Wiederverwendung für vernetzte Produkte

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

Contents

Page

European foreword

This document (prEN 17927:2022) has been prepared by Technical Committee CEN/JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

Introduction

This document specifies the Security Evaluation for Secure IoT Platforms (SESIP). It includes general requirements for Security Functional Requirements (SFRs), Security Process Packages (SPPs) and Security Assurance Requirements (SARs) designed to be used in the evaluation and certification of IoT platforms.

SESIP is a methodology for the security evaluation of platform on which of connected products are based. The term “platform” in SESIP is defined as the implementation of underlying features for an application layer; a platform can be subdivided in “platform parts”.

SESIP does not address the final connected product itself, but the results of the SESIP evaluation of connected platform are meant to be able to be used as evidence for compliance demonstration to standards addressing Connected Products.

This make SESIP not redundant with current IoT standards but a tool on which those standards can base on by reusing outputs. It is indeed impossible for a product vendor to provide, with reasonable effort, assessment evidences for all platform parts integrated from different developers/manufacturers.

This SESIP methodology specific goals are summarized below:

- To be accessible to all IoT products stakeholders;
- To provide clear but harmonized security claims;
- To consider time-to-market needs by providing an optimized and efficient methodology;
- To enable the reuse of evaluation results in different products and/or between different standards and avoid redundant evaluations of same platform (parts)without added value;
- To support Connected Products compliance demonstration to Connected Product standards.

Fulfilling of these goals allows SESIP raising the overall security in IoT ecosystems by increasing the number of security evaluations through clarity in security claims and optimized efforts.

1 Scope

This document describes a cybersecurity evaluation methodology, named SESIP, for platforms and platform parts of connected IoT products. Security claims in SESIP are made based on the security services offered by those platforms. Platform parts can be in hardware and software. SESIP aims to support comparability between and reuse of independent security evaluations. SESIP provides a common set of requirements for the security functionality of platform parts which apply to the foundational platforms of devices that are not application specific. The methodology describes the re-use of evaluation results.

2 Normative references

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

ISO/IEC 17000:2020, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17065:2012, *Conformity assessment — Requirements for bodies certifying products, processes and services*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 17000:2020, ISO/IEC 17065:2012 and the following apply.

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

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1
composite platform
platform integrating a certified platform (part)

3.2
connected application
application
overall software layer implementing an IoT end-user use case based on the underlying connected platform

3.3
connected application part
application part
subset of the connected application defined by a specific context (e.g. data, resources, etc.) and to be isolated from the rest of the application

3.4
connected platform
platform
hardware and/or software that provides secure services to a connected application

3.5
connected platform developer
platform developer
developers who build platform (parts) and supply them to product vendors or to other platform developers, and who need to certify the security of the platform (parts) that they build.

3.6
connected platform part
platform part
part
hardware and/or software that implements a subset of the features of a connected platform, and that can be evaluated separately e.g. the hardware, a cryptographic library, an OS.

3.7
connected product
product
combination of a connected platform and a connected application that a product vendor puts on the market.

3.8
keystore
repository in which certificates, private keys, or secrets can be stored.

3.9
SESIP profile
security profile generic to a type of platform (part), template for a SESIP Security Target of a platform of type targeted by the profile

3.10
SESIP Security Target
SESIP ST
ST
statement of SESIP security requirements in terms of security features (SFRs and SPPs) and evaluation activities (SARs) to be addressed during the evaluation of a platform (part)

4 Overview

4.1 General

This clause provides an overview of the essential principles underlying SESIP:

- The base concepts of the methodology
- A threat model adapted to the IoT ecosystem
- A life cycle adapted to connected products in the IoT ecosystem
- Reusability, an essential objective of SESIP, in order to handle at an acceptable cost the increasing complexity of the connected platforms that need to be evaluated in the IoT ecosystem
- Accessibility, which is required to encourage product vendors to leverage security features included in evaluated connected platforms; the results of an evaluation is expected be accessible and exploitable by security-proficient developers without the need to be evaluation specialists.
- Security self-assessment in SESIP

4.2 SESIP concepts

SESIP is originated from the ISO 15408 series ([4], [5], [6]), specialized for the evaluation of connected platforms in the context of IoT; it provides the base concepts as follows:

- SESIP keeps the main definitions and high-level concepts introduced in ISO 15408-1 [4].
- SESIP Security Functional Requirements (SFRs) for the security features to be implemented by platforms (parts) and to be evaluated; SESIP does not use the SFR catalogue defined in ISO 15408-2 [5] but keeps the concept of a catalogue of SFRs, specialized for the IoT ecosystem, but each SFR being at a level of final service to the user.
- SESIP Secure Process Packages (SPPs) for the security processes to be implemented by the developer of the platform under evaluation.
- SESIP Security Assurance Requirements (SARs) for the evaluation activities to be performed; SESIP keeps the categorization of the Security Assurance Requirements and the associated type of developer's inputs as in ISO 15408-3 [6], however it redefines the content as described in 7.1.
- SESIP assurance levels; SESIP does not use "EAL" packages defined in ISO 15408-3 [6], but defines its own assurance packages adapted to the IoT ecosystem: the SESIP levels (see Clause 8).

See details about SESIP implementation of those concepts in Clauses 5 to 8.

SESIP is an evaluation methodology that defines as precisely as possible how to evaluate the security of a product, in this case a connected platform. Similarly, SESIP does not define any specific procedure, nor does it explicitly organize the mutual recognition principles between certificates, and only provides guidance and directions. A SESIP evaluation/certification scheme based on this SESIP evaluation methodology is expected to be defined in another document by the certification scheme owner.

4.3 IoT use cases and threat model

4.3.1 General

IoT is a broad term, but always contains a product ("thing") and some form of connectivity ("internet"). SESIP focuses on the "thing" side of IoT, and on the security of connected platforms, on which Connected Products are based.

4.3.2 Architecture

A Connected platform typically includes the following components:

- Hardware (processing unit, memory, possibly a secure element, at least one network interface, possibly some sensors) and associated features e.g. Firmware, Boot Loader and Root-of-Trust.
  - o It is assumed that the connected platform includes at least one network interface that is directly or indirectly connected to a network and exposed to potential attackers.
- An operating system, providing a foundation to run Connected Applications on the hardware.
- A network connectivity layer (e.g. Comm library), allowing the connection of the product to backend or other products.
- Software application services offered to Connected Applications, providing an application framework to product vendors (e.g. Crypto library, Secure Storage, Identity and Attestation features).

The Figure 4-1 shows an example of a Connected platform:

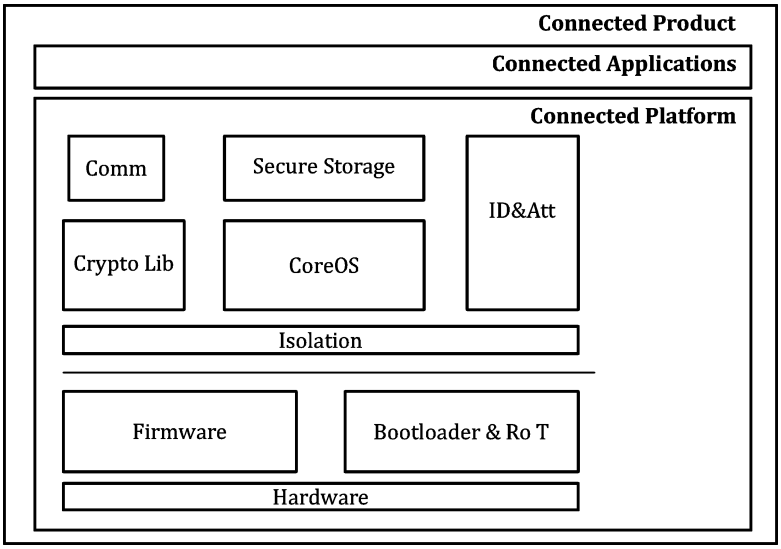


Figure 4-1 — Example of connected product architecture

4.3.3 Assets

Platform assets depend on the platform implementation and use case. However, the list of typical main assets shown in Table 4-1 has been established by a group of IoT stakeholders:

Table 4–1 — Main assets of connected platform

Asset	Protections
User data (local)	Privacy concerns are essential. Protections of confidentiality, integrity and authenticity shall be provided.
User data (authentication data)	Confidentiality is required for secrets. Secondary data (like counters) shall be appropriately protected (confidentiality, integrity).
Data in transit (internet)	Confidentiality and integrity are often essential, as is the authenticity.
Data in transit (local)	Integrity is often essential. Confidentiality is not a systematic requirement. Authenticity is less common.
Code, including platform code and application code	Integrity and authenticity are strong requirements. Confidentiality is optional.
Product identity	Integrity and unicity are required.
Configuration and system data	Integrity and authenticity are required.
Life cycle related data	Integrity is required.

It is understood that not all platforms provide complete coverage, but such limitations shall be carefully motivated when claiming SESIP SFRs (e.g. limited bandwidth or legacy protocol).

The assets may be further categorized into different criticality levels that will be protected at the appropriate level in the platform (part) – in the case of a multi-assurance platform, see 4.5.2. For instance, there may be different levels of cryptographic keys, depending on their function and life cycle. In that case:

- Protection mechanisms shall be appropriate at every level.
- Assets shall be usable without disclosing them to a lower level.
- Usage of the assets from a lower level shall be appropriately controlled (access control).

4.3.4 Attackers and threats

4.3.4.1 Base scenario

The minimum and mandatory threat model in SESIP is an attacker with only remote (no physical) access to the connected platform during the exploitation phase (see Annex B). This addresses the main IoT concern of a scalable attack exploited using a remote connection to the connected platform.

Nevertheless, the attacker can perform any type of preliminary attack on a connected platform (part) owned, including physical attacks; this shall be considered for the base scenario in an identification phase (see Annex B).

Also, in this base scenario, threats related to untrusted software that could be loaded onto connected platforms are not considered.

4.3.4.2 Extended scenario – physical access

When connected platforms are physically accessible to attackers, the threat model can be expanded and covered by the use of the SFRs "Limited physical attacker resistance" and "Physical attacker resistance". The typical example scenarios where attackers have physical access to a victim product are:

- Connected platform deployed outside of a physically protected environment; e.g. a doorbell, outside IP camera.
- Temporary physical access; e.g. "evil maid" attacks where the attacker has temporary physical access to the product that has already been acquired by an end user, or "supply chain" attacks where the attacker delivers a compromised product to the target.

4.3.4.3 Extended scenario – untrusted software

When untrusted software can be loaded onto connected platforms, either by the end user or by an external entity, and that could impact the platform, its parts, or its applications, the base threat model can be expanded and covered by the use of the SFRs "Software attacker resistance: Isolation of platform", "Software attacker resistance: Isolation of platform parts", and "Software attacker resistance: Isolation of application parts".

4.4 Connected product life cycle

Different life cycle models can be applied to Connected Products, and to the connected platforms that compose each product. Nevertheless, some patterns can be found in most products that are significant for security:

<u>Vendor provisioning</u> is the phase during which the product is provisioned with credentials that are shared with the vendor's backend, and that allow the product to communicate securely with the backend and to perform management operations. This phase typically concludes with the delivery of the product to the customer.

User provisioning is the phase during which the product is provisioned with a user's credentials and specific data that allow the product to represent that user. This phase typically concludes with the normal usage phase of the product.

Normal usage is supposed to be the product's normal state, until one of the following events occurs:

- The user applies a factory reset, which removes all user-related data and credentials, and prepares the product to be transferred to another entity (e.g. for resale, for return, or even for temporary storage). The product is then ready again for user provisioning, but a user should not have the ability to return the product to an earlier life cycle phase.
- The user decommissions the product, before discarding it. This Terminated state is irreversible.

Some products may include an additional state related to Field return, during which specific debugging features may be available. All user data and credentials shall have been removed before reaching that state.

The product life cycle shown in Figure 4-2 is used as a reference in the SFRs when references to a life cycle are required.

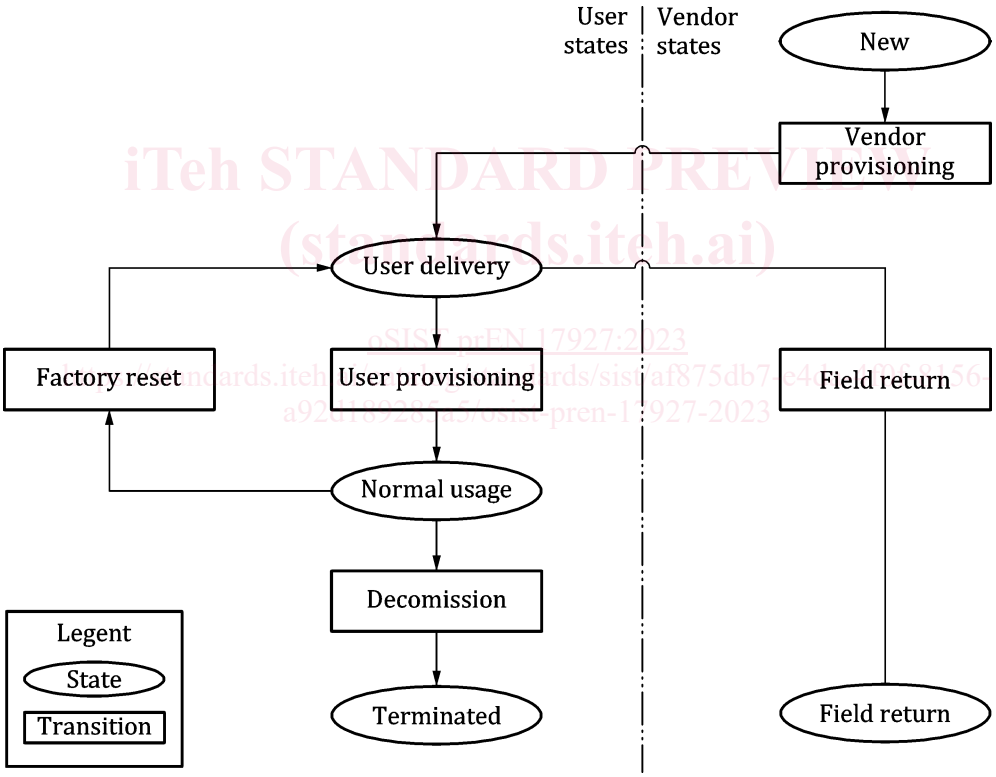


Figure 4-2 — Reference product life cycle

Note that the vendor states are only reachable by the vendor, either before delivery of the product, or after return of the product by the user.

In addition to the product life cycle, the connected platform and some of its parts may have different life cycles that are also significant to security. Such security life cycles are product-specific, and their contribution to the security of the connected platform (part) should be described in the corresponding Security Target.

4.5 Reusability in SESIP

4.5.1 General

Connected Products are complex, often much more than most of the products that have had their security formally certified until today. SESIP recognizes this by providing a dedicated methodology for the connected platforms on which these products are based. connected platforms are often built by assembling several pre-existing hardware and software components; some of them include security components that protect critical assets and need to be evaluated at a high assurance level. Such components are often integrated in several connected platforms targeting different use cases.

SESIP methodology defines ways to independently evaluate subsets of components, which may then be called platform parts, and reuse the evaluation results in any connected platform. Those results can come from an evaluation under SESIP methodology, but also from other compatible external evaluations.

4.5.2 Building connected products from connected platforms

4.5.2.1 Reuse of external evaluations

As mentioned in 4.3, SESIP focuses on the "Things" in IoT, and more specifically on the solutions on which these connected things are built, which we call Connected Products. Every Connected Product belongs to a category or a vertical, and dedicated security standards are likely to be built for the most common types of Connected Products (e.g. Consumer IoT, Industrial IoT, Connected Vehicles, etc.). For each type, a specific risk analysis is needed to determine the appropriate functional and assurance requirements and may then result in the creation of a specific evaluation scheme.

In such a multi-scheme context, the SESIP methodology security requirements are defined in a way that enables the establishment of equivalence with the requirements of other schemes. After successful compatibility analysis, this allows the reuse of evaluation results between schemes.

4.5.2.2 Reuse of platform parts evaluations

4.5.2.2.1 General

A typical connected platform is not a monolithic component, as it comprises some hardware, including at least one [micro]controller or [micro]processor, and some software, including at least an operating system. A connected platform may include many more components, for instance related to communication or security. A vendor typically builds its connected platform by selecting hardware and software components, most likely from different third-party vendors, and then assembling them.

Every vendor in that supply chain needs to provide security evaluation assessment, ending with the integrator in charge of ensuring that the full connected platform is secure. To maintain security through the whole assembly process can be quite complex, unless all the vendors of those components (hardware and software) use a common methodology.

In order to address this, SESIP considers the following reuse contexts:

- Reuse of evaluated platform parts in several platforms (parts)
- Reuse of evaluated platform parts from a hosting platform (part) to another one

4.5.2.2.2 Reuse of evaluated platform parts in several platforms (parts)

SESIP allows the evaluation of platform parts, individually or in composition (see 4.5.3), in such a way that the evaluation results of those platform parts remain applicable in different Connected Products.

An example is provided in Figure 4-3:

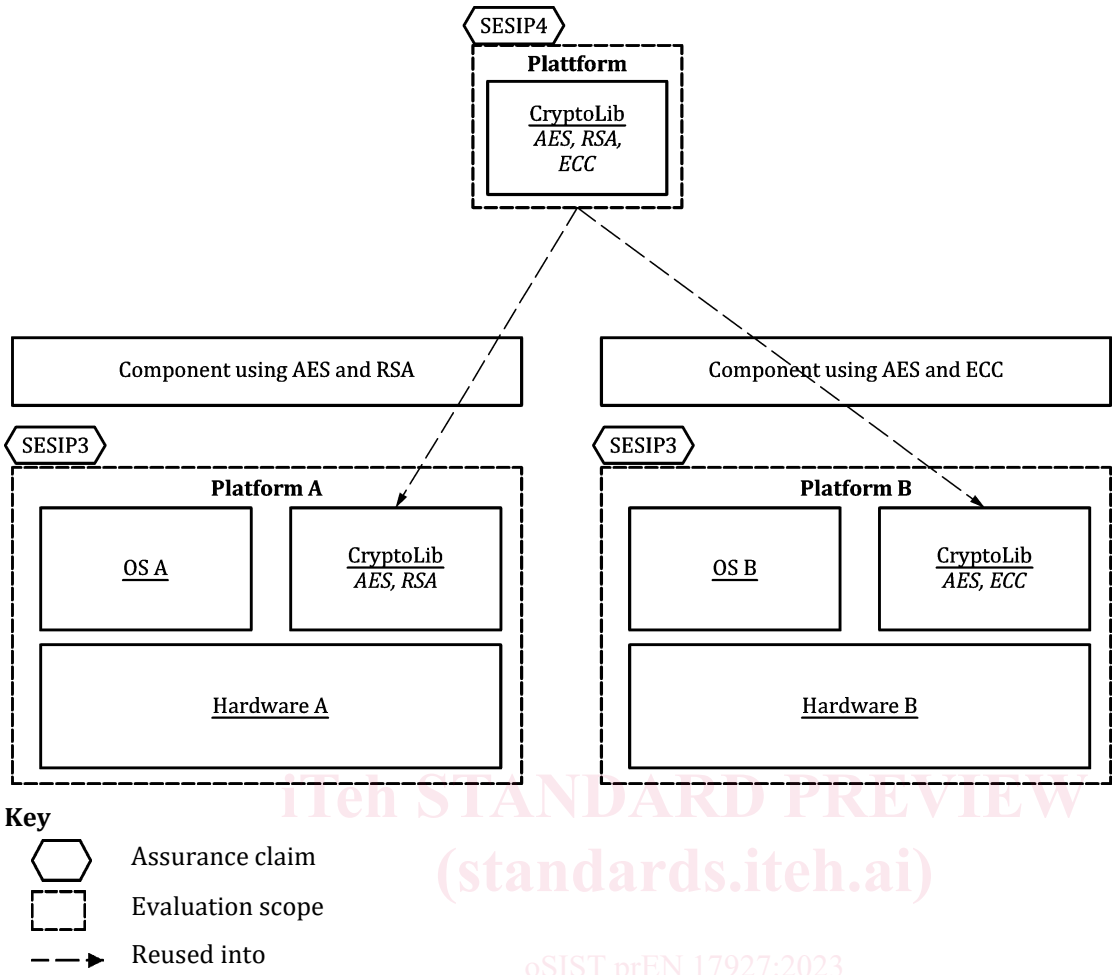
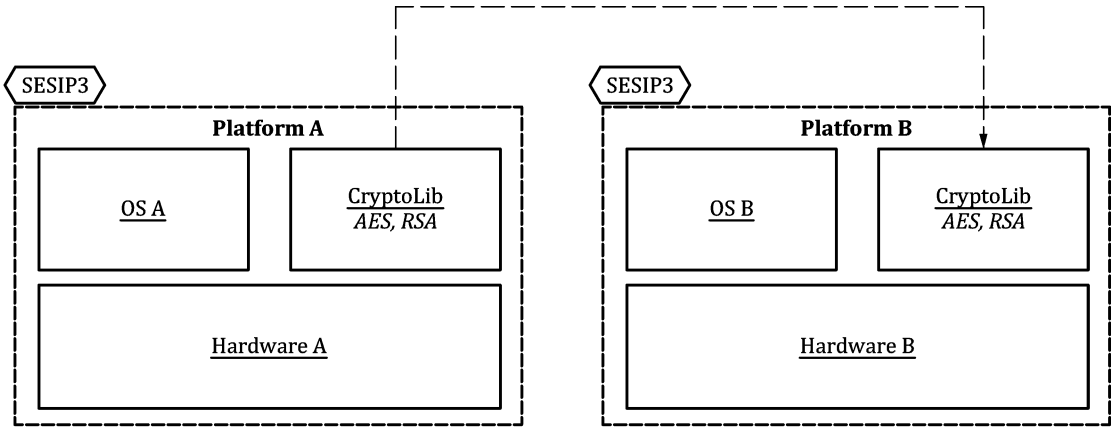


Figure 4-3 — Example of evaluation results reuse in several platforms (parts)

4.5.2.2.3 Reuse of evaluated platform parts from a hosting platform (part) to another one

Another case of reuse allowed by SESIP: When a part has been evaluated inside a particular platform (part), the related evaluation results can be reused for integration into another platform (part).

An example is provided in Figure 4-4:



Key

Assurance claim

Evaluation scope

Reused into

Figure 4-4 — Example of evaluation results reuse from a platform (part) to another one

In all cases, the reuse of evaluation evidences is in particular based on security integration guidance for each component; then, the assessment of the connected platforms integrating evaluated platform parts requires the verification that secure integration guidelines and composition rules (see 4.5.2) are respected.

Note that reuse effort will vary depending on the use case, from straightforward portability with few verifications, e.g. full self-containment of security functionality, to a dedicated set of activities needing to be performed on the integrating scope and to be defined in the previously mentioned integration and composition guidelines. In any case, the effort will be significantly lower than a re-evaluation on evaluated parts in a new platform (part).

Using SESIP as core methodology allows vendors to have a clear understanding of the assumptions and guidance of the third-party components they integrate by reusing evidences provided by the components' vendors during the evaluation of their platform (part).

4.5.2.3 Reuse of platform evaluation in connected products

Most Connected Products will be built by vendors who develop one or several dedicated Application(s) on top of a generic or off-the-shelf connected platform. SESIP focuses on the connected platform to provide a foundation for the security assessment, and potentially the certification, of Connected Products. It addresses the security level of the whole operating system including services used for the storage, installation, initialization, and execution of this Application, as well as its data protection.