Global Platform®

Securing the digital future

GlobalPlatform Technology

SESIP Profile Approval Process

Version 1.0

Public Release

May 2026

Document Reference: GPS_GUI_030

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

Tables

Figures

1 INTRODUCTION

This document outlines the approval process for SESIP Profiles developed by various entities, both within and outside of GlobalPlatform. This process ensures that each SESIP Profile meets the highest standards of quality and aligns with GlobalPlatform's stringent requirements.

Upon successful completion of this process, the SESIP Profile will be officially announced and granted the right to display the SESIP logo, which signifies compliance and trustworthiness in the realm of security evaluation.

1.1 Audience

This document is intended for developers of SESIP Profiles, as well as for reviewers of SESIP Profiles: the SESIP Technical Working Group for profiles developed within GlobalPlatform and SESIP Certification Bodies (CBs) for profiles developed externally.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that has been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

Table 1-1: Normative References

Standard / Specification	Description	Ref
GP_FST_070	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP) Methodology v1.2, July 2023	[SESIP]
EN 17927	Security Evaluation Standard for IoT Platforms, November 2023	[EN 17927]
GP_GUI_067	SESIP Governance v1.2	[SESIP Gov]
	SESIP Security Target Template v2.2 https://trustcb.com/download/sesip-security-target-template-v2-2	[SESIP ST]

Table 1-2: Informative References

Standard / Specification	Description	Ref
GP_GUI_001	Document Management Guide	[DMG]

1.4 Terminology and Definitions

Selected terms used in this document are included in Table 1-3.

Table 1-3: Terminology and Definitions

Term	Definition
Platform	In the context of this document, equivalent to Connected Platform, as defined in [SESIP].

1.5 Abbreviations

Table 1-4: Abbreviations

Abbreviation	Meaning
CB	Certification Body
SAR	Security Assurance Requirement
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirement
ST	Security Target

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and clarifications; all non-trivial changes are indicated, often with revision marks.

Table 1-5: Revision History

Date	Version	Description
May 2026	v1.0	Public Release

2 OVERVIEW

2.1 Scope

The process specified in this document applies to SESIP Profiles developed both within GlobalPlatform and by external entities. It covers the evaluation, approval, and formal recognition of SESIP Profiles to ensure alignment with GlobalPlatform's security standards. Successful completion of this process entitles the SESIP Profile to use the GlobalPlatform SESIP logo.

The process applies to:

- Newly developed SESIP Profiles seeking approval
- Revisions and updates to existing SESIP Profiles

2.2 Objectives

The aim of this process is to establish an approval framework for SESIP Profiles, ensuring that they:

- Align with GlobalPlatform's technical and compliance requirements.
- Meet expected quality.

Consistent use of this process will:

- Ensure consistency and reliability in SESIP Profiles.
- Enhance recognition and credibility by granting the SESIP logo, signifying compliance and trustworthiness.
- Facilitate mutual SESIP certificate recognition between SESIP Certification Bodies (CBs).
- Ensure that SESIP Profiles contribute to a robust, scalable, and interoperable security evaluation ecosystem.

2.3 Roles and Responsibilities

To ensure the effectiveness and quality of the SESIP Profile approval process, the following roles are defined, each with distinct responsibilities:

- **SESIP Profile Developer**: Responsible for authoring SESIP Profiles in accordance with this document, and for addressing feedback from the approval process.
- **SESIP Profile Reviewer**
  - For GlobalPlatform developed SESIP Profiles, the SESIP Technical Working Group is the reviewer. For externally developed SESIP Profiles, a Certification Body (CB) is the reviewer.
  - Responsible for reviewing SESIP Profiles and ensuring that they meet all defined requirements.
- **SESIP Profile Publisher**: GlobalPlatform publishes the approved SESIP Profile at the GlobalPlatform SESIP official repository.

3 SESIP PROFILE

3.1 Purpose of the SESIP Profile

A SESIP Profile is specifically designed to specify the security requirement of a specific use case or operational environment. It defines the minimum set of security requirements to be implemented by a type of product to ensure a reasonable level of security regarding relevant threats. Note that threats are identified by the stakeholders of the specific products.

3.2 Key Components of the SESIP Profile

Each Security Functional Requirement (SFR) defined in the profile should directly address a specific security threat or challenge within the system. The SFRs shall be clearly mapped to identified threats, ensuring that they provide effective mitigation strategies and contribute to the overall security posture of the evaluated product or system.

In SESIP methodology, SESIP Security Targets are required to identify Security Functional Requirements (SFRs), but threat analysis is out of the scope of security evaluations. This is a full process that needs to be performed by experts of the product type. It is left to the stakeholder community of a product to identify the threats to be covered and how. However, knowledge of threats and use cases covered by the selection of SFRs can be highly useful to the reader.

3.2.1 Conformance Claims/SESIP Level(s) Claim

The SESIP Profile shall explicitly state conformance to one or more SESIP Levels. This conformance ensures that the profile aligns with the security objectives and assurance requirements of the chosen SESIP Level(s). Each SESIP Level has distinct security and evaluation criteria, and the profile shall define how it meets the corresponding functional, assurance, and security testing requirements.

The conformance claim shall be included and justified as part of “Mapping And Sufficiency Rationales” section of the profile (see section 5 on page 11).

3.2.2 Required Sections in the SESIP Profile

The SESIP Profile shall include the following key sections to ensure a structured, comprehensive, and consistent security evaluation approach, aligning with the SESIP Security Target template ([SESIP ST]). Each section is outlined below with detailed descriptions of its content and purpose:

1. INTRODUCTION

This section provides a high-level introduction to the concept of a SESIP profile.

Example:

> The Security Evaluation Standard for IoT Platforms ([SESIP]) defines general requirements for Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that are intended for use in evaluating and certifying platforms. A SESIP Profile represents a generic security profile for a specific type of platform (part). It outlines the SESIP requirements in terms of security features and evaluation activities that must be addressed during the evaluation of a platform (part) of the targeted type.
>
> This document provides the SESIP Profile applicable to security evaluations of < Platform type name >.

1.1 SESIP Profile Reference

This section should identify clearly the profile.

SESIP Profile Name	
SESIP Profile Version	
Platform Type	

Security Targets claiming and achieving conformance to this profile should show < logo > to indicate this.

1.2 References

- Lists all relevant standards, guidelines, and regulatory requirements referenced in the profile.
- Ensures consistency and traceability with established security frameworks.

1.3 Terminology and Definitions

- Defines key technical terms, acronyms, and security-related terminology used in the profile.
- Ensures a clear and common understanding for reviewers, developers, and stakeholders.
- May reference industry-standard glossaries, such as those from ISO/IEC, CEN/CENELEC, or NIST.

1.4 Revision History

- Tracks changes and updates made to the profile.
- Ensures transparency in the evolution of the SESIP Profile.

2. PLATFORM FUNCTIONAL OVERVIEW AND DESCRIPTION

- Provides a comprehensive description of the platform type, including its architecture, components, and security features.
- Defines the scope of the SESIP Profile in terms of functionality, intended use cases, and security boundaries.
- May include a block diagram or architecture diagram illustrating the platform's components and interactions.
- (Optional) Highlights any pre-existing certifications or compliance efforts related to the platform.

3. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security goals that shall be met within the operational environment where the platform is deployed.

3.1 Security Objectives for the Operational Environment

Specifies the security responsibilities and expectations for the platform within its intended deployment scenario.

3.2 (Optional) Inherited Objectives for the Operational Environment

Specifies the security responsibilities and expectations for the platform within its intended deployment scenario, mainly in composition evaluation.

4. SECURITY REQUIREMENTS

This section specifies the Security Assurance Requirements (SARs) and Security Functional Requirements (SFRs) that the platform shall meet.

4.1 Security Assurance Requirements (SARs)

- Defines the evaluation and assurance requirements needed to verify that the platform meets its security claims.
- Aligns with the SESIP Level(s) claimed.

4.2 Security Functional Requirements (SFRs)

- Lists the specific security functions that the platform shall implement.

4.3 Security Process Packages (SPPs)

- Lists the specific security processes that the platform shall implement to mitigate identified threats (see [EN 17927]).

5. MAPPING AND SUFFICIENCY RATIONALES

This section provides a detailed mapping of the following:

5.1 SESIP Level(s) Sufficiency Rationale

Justification for selecting the SESIP Level based on the threat landscape and risk assessment should be presented.

A detailed explanation of how the profile meets the Security Assurance Requirements for the claimed level(s).

Table 3-1 provides an example that can be followed. (A full description can be found in [EN 17927], Annex D.6.2.)

Table 3-1: Example SESIP Level Sufficiency Rationale

Assurance Category	Assurance Requirements	Covered by	Rationale
ASE: Security Target Evaluation	ASE_INT.SESIP	Section “Platform Functional Overview and Description”	Provides the generic description for the platform type. The compliant ST shall adapt the description to its specific platform.
	ASE_OBJ.SESIP	Section “Security Objectives for the Operational Environment”	Lists the security objectives to be fulfilled by the platform environment. The compliant ST shall integrate at minimum all those security objectives or equivalent.
	ASE_REQ.SESIP	Section “Security Requirements”	Lists the SESIP requirements (SARs, SFRs, SPPs). The compliant ST shall integrate at minimum all those requirements.
	ASE_TSS.SESIP	Sections “Security Functional Requirements” and “Security Process Packages”	The compliant ST shall provide the rationale of how the SFRs and SPPs are met.

5.2 Mapping(s) with External Standards

Demonstrates compliance with SESIP standards, ensuring that reviewers, regulators, and stakeholders can confidently assess the platform’s security posture.

4 SESIP PROFILE VERIFICATION TASKS

To ensure the correctness and consistency of a SESIP Profile, a set of checking tasks must be performed against each item specified in section 3.2.2. These tasks form the backbone of quality assurance and provide confidence that the profile adheres to SESIP methodology and industry expectations.

These verification tasks should be systematically executed and documented as part of the SESIP Profile evaluation process. Addressing them not only strengthens the credibility of the profile but also supports smoother progression through the approval workflow detailed in subsequent sections of this document.

The SESIP Profile Verification Tasks should detail the essential checks required to ensure the accuracy, completeness, and quality of the SESIP Profile. These tasks can be outlined as follows:

- **Scope Validation**: Ensure the profile clearly outlines its scope, including the target platform, its boundaries, and intended use cases. All relevant functional, logical, and physical aspects should be precisely described.
- **SFR and SAR Mapping**: Check that Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) are comprehensively mapped. Every requirement should be traceable and consistent with SESIP standards.
- **Assumptions and Environment**: Confirm all operational assumptions and environmental conditions are explicitly stated, justified, and match the deployment context for the profile.
- **Rationale and Justification**: Review the rationale provided for each profile element to ensure justifications are logical, well-founded, and meet the SESIP Level.
- **Consistency and Completeness**: Perform a cross-check to ensure all sections use consistent terminology and that no required items are missing.
- **Documentation Quality**: Evaluate the clarity and organization of the documentation, ensuring tables, diagrams, and cross-references are accurate and easy to follow for auditors and stakeholders.

These verification tasks, when systematically carried out and documented, are crucial for validating the SESIP Profile and supporting its approval process as described in subsequent sections.

5 SESIP Profile Approval Flow for Internally Developed Profiles

The SESIP Profile approval process for internal developments submitted through the SESIP Technical Working Group will follow the GlobalPlatform publication approval workflow, as described in GlobalPlatform's Document Management Guide ([DMG]).

6 SESIP Profile Approval Flow for Externally Developed Profiles

The SESIP Profile approval process follows a structured path to ensure the security profile meets industry standards and compliance requirements.

The initiator and sponsor of the process is the profile developer(s).

Each externally developed SESIP Profile must be evaluated and approved by a SESIP Certification Body before being published by GlobalPlatform.

Figure 6-1: SESIP Profile Approval Flow

Below is a detailed breakdown of each stage:

A. Develop the SESIP Profile

The developer drafts the SESIP Profile according to section 3.

Outcome: A draft SESIP Profile ready for evaluation.

B. Submit to Certification Body

The developer formally submits the completed SESIP Profile to the Certification Body (CB) for evaluation.

Outcome: The profile is officially in the evaluation process.

C. Certification Body Review

The Certification Body reviews the profile in depth, ensuring conformance with the SESIP requirements. This includes:

- Assessing compliance with SESIP Levels (i.e., Level 1–5).
- Reviewing for clarity, completeness, and alignment with security requirements.
- Verifying the mapping of security requirements.

Outcome: The profile is either accepted for final evaluation or returned for revisions.

D. Certification Body Decision

Once the final evaluation is complete, the Certification Body makes a decision:

- If the profile meets SESIP requirements, the Certification Body issues SESIP approval notification, authorizing the use of the GlobalPlatform logo and QR code.

Outcome: Approved SESIP Profile, ready for industry use.

E. Publication

After approval, the approved SESIP Profile is publicly registered:

- The profile is added to the GlobalPlatform SESIP official repository, ensuring public accessibility.
- Industry stakeholders, product developers, and Certification Bodies can reference the Profile for compliance and integration.
- It serves as an authoritative security profile for products using SESIP guidelines.

Outcome: The SESIP Profile is officially recognized and accessible for industry adoption.

F. Ongoing Maintenance

To maintain relevance, the developer should monitor and update the profile:

- Periodically reviewing security requirements based on new threats and industry changes.
- Implementing necessary updates and modifications.
- Collaborating with the Certification Body for approval of major revisions.
- Ensuring that security measures remain effective and aligned with evolving cybersecurity standards.

Outcome: A continuously maintained and updated SESIP Profile, ensuring long-term security compliance.

7 SUMMARY

The SESIP Profile approval process ensures standardized, reliable certification for IoT platforms. It enhances clarity and consistency in defining security requirements, aligns with industry best practices, and ensures compliance with SESIP Levels. The structured evaluation strengthens trust and credibility, while the final certification and publication provide industry recognition. Ongoing maintenance ensures adaptability to emerging threats, making the SESIP framework a robust and future-proof security solution.