Global Platform®

The standard for secure digital services and devices

GlobalPlatform Technology

SESIP Governance

Version 1.2

Public Release

September 2024

Document Reference: GP_GUI_067

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 describes the governance process for the Security Evaluation Standard for IoT Platforms (SESIP). The document specifies the competencies and accreditations required for the Certification Bodies and for the Laboratories performing evaluation activities, and the process that a Certification Body shall follow to issue a certificate of compliance.

The use of this document will facilitate cooperation between Laboratories and Certification Bodies, and assist in the exchange of information and experience, and in the harmonization of standards and procedures. The acceptance of results between countries is facilitated if Laboratories conform to this document.

This document is structured as follows:

- Section 2 introduces the document scope.
- Section 3 deals with Certification Body licensing requirements.
- Section 4 deals with Evaluation Laboratory licensing requirements.
- Annex A lists the minimum content of SESIP certificates.

1.1 Audience

This document is intended primarily for the use of all stakeholders of the security evaluation of Connected Platforms. This document is applicable to all organizations performing SESIP activities under GlobalPlatform licensing.

Laboratory customers, regulatory authorities, organizations and schemes using peer-assessment, Accreditation Bodies, and others use this document in confirming or recognizing the security level of Connected Platforms.

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 have 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

The table below lists references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: Normative References

Standard / Specification	Description	Ref
ISO/IEC Guide 99:2007	International vocabulary of metrology – Basic and general concepts and associated terms (VIM)	[ISO Guide 99]
ISO/IEC 15408-3:2008	Information technology – Security Techniques – Evaluation criteria for IT security – Part 3: Security assurance components	[ISO 15408-3]

Standard / Specification	Description	Ref
ISO/IEC 17000:2004	Conformity assessment – Vocabulary and general principles	[ISO 17000]
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories	[ISO 17025]
ISO/IEC 17065:2012	Conformity assessment – Requirements for bodies certifying products, processes and services, September 2012	[ISO 17065]
GP_FST_070	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP) Methodology	[SESIP]
Application of Attack Potential for Smart Cards	Application of Attack Potential for Smart Cards, latest version	[AAP]

1.4 Terminology and Definitions

Selected terms used in this document are included in Table 1-2. Additional terms are defined in [ISO 17000].

Table 1-2: Terminology and Definitions

Term	Definition
Certification Body (CB)	Throughout this document the term “Certification Body” is used in keeping with the terminology of [ISO 17065], and holds the same meaning as “Conformity Assessment Body” as defined in [ISO 17000].
Certification Scheme	Certification system related to specified products to which the same specified requirements, specific rules and procedures apply ([ISO 17000]). A scheme may be developed among others by a Certification Body or by a “scheme owner” representing a specific group of interests. The scheme may contain requirements on Conformity Assessment procedures and functions of the Certification Bodies complementary to those established by [ISO 17065].
Conformity Assessment	Demonstration that specified requirements relating to a product, process, service, person, system, or body are fulfilled.
Evaluation Laboratory, Laboratory	As defined in [ISO 17025], a body that performs one or more of the following activities: testing, calibration, sampling associated with subsequent testing or calibration.
Requirement	Expression in the content of a document conveying objectively verifiable criteria to be fulfilled and from which no deviation is permitted if compliance with the document is to be claimed.

1.5 Abbreviations and Notations

Table 1-3: Abbreviations and Notations

Abbreviation / Notation	Meaning
CB	Certification Body
CC	Common Criteria
SESIP	Security Evaluation Standard for IoT Platforms

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 1-4: Revision History

Date	Version	Description
Jun 2020	0.0.0.5	Member Release
Jul 2022	1.0	Initial Public Release
Dec 2022	1.1	Public Release • Added the process for managing Certification Body (CB) recognition (section 3.2.3).
Sep 2024	1.2	Public Release • Added section 4.2.2 on upgrading from SESIP2 to SESIP3 requirements. • Added the Certificate QR code (section A.3). • Updated section 3.2.3.1 re best agreement for recognition.

2 DOCUMENT SCOPE

The SESIP standard has been designed to be used under a Certification Scheme able to demonstrate compliance under the requirements of the different SESIP assurance levels defined in [SESIP].

The SESIP Governance document has been drafted using the ISO/IEC [ISO 17065] as a guidance. This document provides information and supplementary licensing requirements to enable accreditation bodies to harmonize their application of the standards against which they are bound to assess Certification Bodies. This is an important step towards mutual recognition of accreditation worldwide. It is intended that this Standard should also be useful to Certification Bodies themselves and to those whose decisions are guided by their certificates.

The requirements against which conformity is determined are found in [ISO 17065] and [ISO 17025]. SESIP does not include the text of [ISO 17065] and [ISO 17025] respectively, and users shall purchase those documents from the appropriate Standards organization.

3 CERTIFICATION BODY LICENSING

3.1 Licensing Scope

GlobalPlatform SESIP Certification Body licensing will be provided for a specific technical domain and defined SESIP attacker resistance context and assurance levels (see [SESIP] sections 3.4 and 4 respectively).

The technical domains are not pre-determined, but will be agreed on a case-by-case basis between the GlobalPlatform SESIP licensing secretariat and the Certification Body candidate.

The table below shows the accreditations or equivalent required for each SESIP assurance level. Note: Each level N+1 requires the skills from level N.

Table 3-1: Accreditation vs. SESIP Levels for Certification Bodies

SESIP Assurance Level	Accreditation or Equivalence	Software Skills	Hardware Skills *(on top of Software Skills)*
SESIP1	CCRA Authorizing or SOG-IS (or future EUCC) Authorizing or 17065 (or equivalent in legacy cases) accreditation with CC scope or SESIP scope	• Software security assessment • State-of-the-art remote attacks • Black box	• State-of-the-art hardware attacks
SESIP2		• Code review capabilities	
SESIP3		• White box	• Vulnerability analysis • Experience performing attacks ahead of the market by 2-5 years (R&D)
SESIP4	SOG-IS/EUCC Accreditation with demonstrated skills in technical domains “Smartcards and similar devices” and/or “Hardware devices with security boxes” 17065 accreditation with SESIP scope	**Follow SOG-IS requirements**	
SESIP5			

3.2 Licensing Requirements

An entity wishing to become a GlobalPlatform SESIP Certification Body must fulfill the following requirements:

- Be a CCRA or SOG-IS (or future EUCC) Authorizing member or have an ISO/IEC 17065 or equivalent accreditation (see details in section 3.2.1)
- Be a GlobalPlatform “full” or “participating” member
- Be actively participating in the GlobalPlatform SESIP standard and interpretations maintenance working groups
- Be actively participating in the GlobalPlatform Attack Expert Working Groups
- Be actively participating in Common Criteria working groups (e.g. JHAS, ISCI WG1, CCDB, ISO SC27 WG) depending on the targeted assurance level
- Apply the SESIP methodology
- Provide proof of expertise in the targeted technical domains (see section 3.1) for more than three years
- When addressing firmware/software parts, demonstrate capacity to assess evaluation laboratories against the targeted technical domain
- Demonstrate expertise in using rating methodology (example: [AAP]) for technical domains
- Present a yearly report (as discussed in section 3.2.2) to the SESIP community
- Apply the recognition rules discussed in section 3.2.3

3.2.1 ISO/IEC 17065 Accreditation

A Certification Body applying for a license for SESIP4 or SESIP5 shall hold a valid ISO/IEC 17065 certificate with the scope of SESIP Certification Scheme, with all assurance requirements of the maximum SESIP level included (see Assurance Level definition in [SESIP] section 4), delivered by a member of the IAF (International Accreditation Forum).

A Certification Body applying for a license for SESIP1, SESIP2, or SESIP3 shall hold such a certificate, or shall hold a valid ISO/IEC 17065 certificate with the scope of CC, delivered by a member of the IAF (International Accreditation Forum).

Since SESIP is based on ISO/IEC 15408, any existing Certification Body with ISO/IEC 15408 scope already on their accreditation has a correlation of capacities and therefore can perform an equivalence by expanding the scope of accreditation.

The Certification Body should open one committee (as defined in [ISO 17065]) to a GlobalPlatform representative to allow review of the following operational details:

- Update if any of the SESIP process
- The complaints and appeals report
- Impartiality rules

3.2.2 Yearly Report

Every year, each SESIP licensed CB shall present to the SESIP community an operation report that includes:

- Licensed Laboratories status
- Products certified
  - Security Profile used
  - Type of product / market
- Certificate revoked / withdrawn with vulnerability details if publicly available
- SESIP evolution proposed following a year of operation

3.2.3 Recognition Rules and Processes

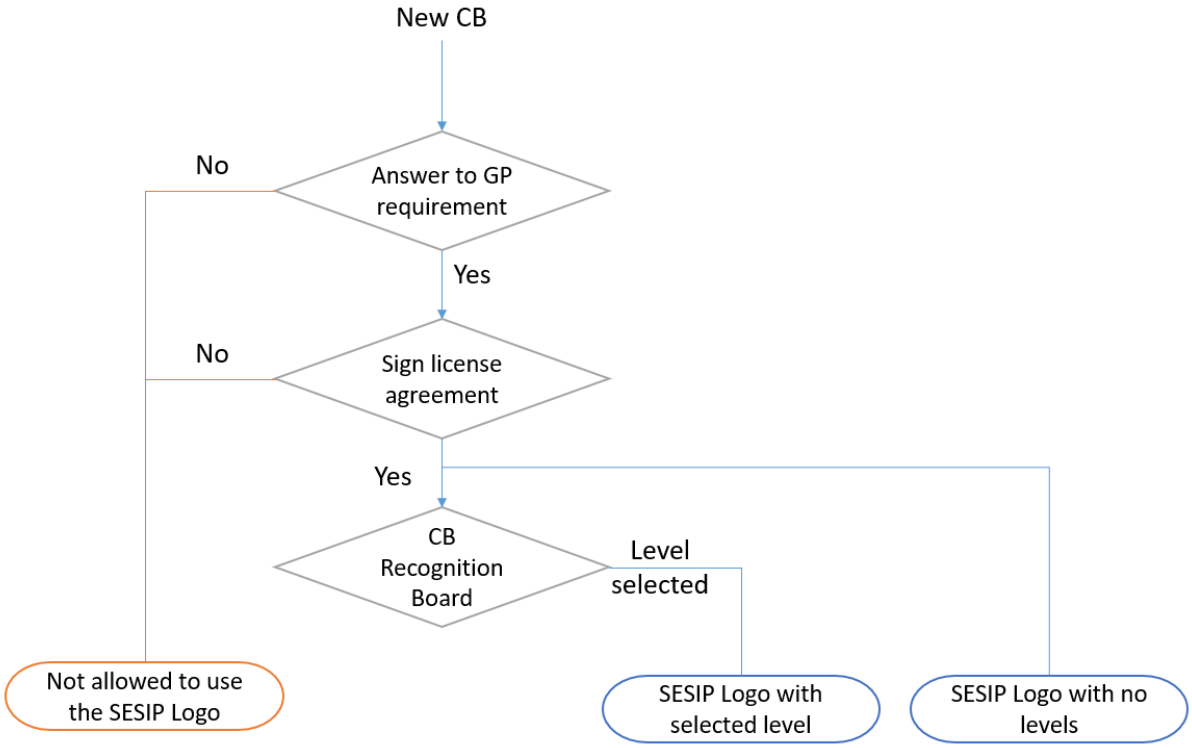
SESIP Licensed CB commit themselves to set up a certificate recognition agreement with all SESIP licensed CBs in accordance with the terms of the:

- GlobalPlatform governance and associated agreements
- Latest version of all technical rules and guidance defined in addition to [SESIP]

3.2.3.1 Process

Regarding onboarding, the figure below shows the main process to manage both the licensing agreement and the certificate recognition agreement.

Figure 3-1: Certification Body Onboarding Process



The CB recognition board allows SESIP Licensed CBs to find the best agreement for recognition, based on at least one completed certification project as basis of the assessment of the quality.

Based on the CB recognition board decision, each licensed CB must sign a one-to-one agreement with a new CB within 12 months of the arrival of a new CB, and the agreement should be reviewed every year.

Notes :

- SESIP logo with no levels indicates that the CB is licensed but the process is not finalized
  - Certificates are not automatically recognized by other CBs
- SESIP logo with selected level –
  - Certificates are automatically recognized by other CBs

3.2.3.2 Peer-to-Peer Review

In order to facilitate the recognition agreement setup and follow up, SESIP licensed CBs should participate to regular peer-to-peer reviews. During peer-to-peer reviews, the new CB must share documents that cover the evaluation and certification scheme process such as but not limited to:

- the yearly report
- the ISO 17065 scope
- the organizational structure of the scheme
- accreditation and licensing policy for labs (ISO 17025, validity, Technical domain)
- if any national set of rules and regulations for evaluation and certification

Such peer-to-peer review will be organized between SESIP licensed CBs based on SESIP levels.

- SESIP 1 and 2:
  - CRA type, verification procedures. E.g. Keep up to date on attacks
  - Check capabilities of the peer
- SESIP 3:
  - SESIP 1 and 2 requirements, plus:
  - Take two example projects, performing a joint study of them
- SESIP 4-5:
  - SESIP 3 requirements, plus:
  - 1:1 engagement among technical domain experts

4 EVALUATION LABORATORY LICENSING

4.1 Licensing Scope

GlobalPlatform SESIP Evaluation Laboratories will be licensed for a specific technical domain and defined security and assurance levels.

The technical domains are not pre-determined, but will be agreed on a case-by-case basis between the Certification Body and the Evaluation Laboratory candidate.

The table below shows the accreditations or equivalent required for each SESIP assurance level. Note: Each level N+1 requires the skills from level N.

Table 4-1: Licensing vs. SESIP Levels for Evaluation Laboratories

SESIP Assurance Level	Accreditation or Equivalence	Software Skills	Hardware Skills *(on top of Software Skills)*
SESIP1	17025 accreditation or similar accreditation with SESIP scope or CC scope National Body recognition	Applied expertise on software security assessment Knowledge of state-of-the-art remote attacks	Knowledge of state-of-the-art hardware attacks
SESIP2		Applied expertise on: • Basic software analysis (e.g. obvious memory corruptions) • Simple Fuzzing (Random Fuzzing) • Tools for reverse engineering, fuzzing, static analysis, dynamic analysis	Applied expertise on: • Standard fault injection; e.g. EMFI, Glitch • Standard Side Channel • Testing printed circuit boards: Chip probing, memory dumping, port deporting • Standard tools listed in the [AAP]
SESIP3	17025 accreditation with SESIP scope or CC scope National Body recognition	Applied expertise on: • Advanced software analysis (e.g. complex memory corruption requiring deep implementation understanding, race conditions, design errors) • Advanced Fuzzing (e.g. Model Based fuzzing) – Fuzzing tool development capabilities	Applied expertise on: • Specialized fault injection; e.g. LFI, BBI • Specialized Side Channel • Applied expertise on testing printed circuit boards: Chip preparation for invasive attacks • Specialized tools listed in the [AAP]

SESIP Assurance Level	Accreditation or Equivalence	Software Skills	Hardware Skills *(on top of Software Skills)*
SESIP4	SOG-IS/EUCC Accreditation+ with demonstrated skills in technical domains "Smartcards and similar devices" and/or "Hardware devices with security boxes" 17025 accreditation with SESIP scope or CC scope	**Follow SOG-IS requirements**	
SESIP5			

4.2 Licensing Requirements

An entity wishing to become a GlobalPlatform SESIP Evaluation Laboratory must fulfill the following requirements:

- Have an ISO/IEC 17025 or equivalent accreditation (see details in section 4.2.1)
- Be licensed under at least one SESIP CB
- Be a GlobalPlatform "full" or "participating" member
- Be actively participating in the GlobalPlatform SESIP standard and interpretations maintenance working groups
- Be actively participating in the GlobalPlatform Attack Expert Working Groups
- For SESIP levels 4 and higher, be actively participating in Common Criteria working groups (e.g. JHAS, ISCI WG1, CCDB, ISO SC27 WG) depending on the targeted assurance level
- Maintain SESIP expertise
- Apply the SESIP methodology
- Provide proof of expertise in the targeted technical domains (see section 4.1) for more than three years
- When addressing firmware/software parts, demonstrate capacity to perform appropriate analysis and testing
- Demonstrate expertise in using rating methodology (example: [AAP]) for technical domains
- Have a minimum of 1M€ assurance contract

4.2.1 ISO/IEC 17025 Accreditation

The Evaluation Laboratory shall hold a valid ISO/IEC 17025 certificate with the scope of SESIP Certification Scheme, with all assurance requirements of the maximum SESIP level included (see Assurance Level definition in [SESIP] section 4), delivered by an ILAC (International Laboratories Accreditation Cooperation) member of the IAF (International Accreditation Forum).

Since SESIP is based on ISO/IEC 15408, any existing Certification Body with ISO/IEC 15408 scope already on their accreditation has a correlation of capacities and therefore can perform an equivalence by expanding the scope of accreditation.

4.2.2 Upgrade from SESIP2 to SESIP3 Requirements

An Evaluation Laboratory accredited to SESIP2 and aiming for a higher level must meet the following minimum requirements:

Evaluation Experience

- Provide records of at least three VAN 2 evaluations conducted in the last two years, with at least one being a hardware (HW) evaluation.

Capability Demonstration

- Demonstrate capabilities as described in section 4.1.

Extended Knowledge, Capabilities, and Skills

- Connected Platform Design
  - Understand Connected Platform-based design and the general IC design and manufacturing process.
- Connected Platform Technology
  - Understand the technology, underlying principles, and development equipment used by Connected Platform manufacturers.
- Hardware Physical Attack Techniques
  - Possess knowledge and experience in techniques that could compromise a Connected Platform, and the ability to use related equipment to stress hardware layers, understanding IC's physical principles per best practices for VAN 2 & VAN 3 (see [AAP]). VAN 4 capabilities, although not required, would be an advantage.
- Physical Disruptions
  - Possess knowledge and experience in techniques that could alter Connected Platform behavior to downgrade IC-based device security. Possess ability to use equipment to conduct physical disruptions and understand their effects on hardware.
- Cryptographic Attack Techniques
  - Possess knowledge and experience in cryptographic attack techniques, with the ability to perform analysis, including data-capture and signal processing, as per GlobalPlatform state-of-the-art methodology.

- ADV_IMP.3 Skills
  - Possess capability to assess the complete mapping of the implementation representation of the TSF to the SFRs.
- Composite Platform Vulnerability Assessment
  - Possess knowledge in assessing vulnerabilities in composite platforms.

Tool Access

- Must have unlimited access to the majority of tools required for performing software (SW) and hardware (HW) attacks, such as side-channel and perturbation attack tools, based on the attack methodology [AAP].

SESIP 3 Accreditation Process

- Should include an evaluation of VAN 3 with physical attack.

By meeting these requirements, laboratories can ensure that they possess the necessary expertise and resources to achieve higher SESIP accreditation levels.

4.3 GlobalPlatform Licensing Process

It is the responsibility of a SESIP licensed Certification Body to ensure that the candidate Laboratory actually meets the licensing requirements listed in section 3.2.

After at least one accreditation by a SESIP licensed CB, the Laboratory should deliver all information during GlobalPlatform membership renewal. Following GlobalPlatform review, a process will provide access to protected logos. GlobalPlatform will take the proper legal steps to enforce the correct use of the trademarks.

GlobalPlatform reserves the right to suspend or revoke the licensing status of a laboratory upon unsatisfactory renewal.

The detailed licensing process will be publicly available on the GlobalPlatform web site.

4.4 GlobalPlatform Laboratory Onboarding Process

GlobalPlatform maintains an onboarding program to support the Laboratory in learning, implementing, and performing SESIP evaluations.

This onboarding program offers a tailored project depending on the initial status of the laboratory and the expected level to reach.

Annex A SESIP CERTIFICATE REQUIREMENTS

A.1 Certificate Minimum Content

Certification Bodies are responsible for issuing SESIP certificates. However, to ensure comparability between SESIP certificates, certain content must be common to all certificates.

This minimum content is listed in the following table.

Table A-1: Certificate Minimum Content

Certification Body Logo	GlobalPlatform SESIP logo including Level and Attacker profile
GlobalPlatform SESIP Certified	SESIP level (SESIPx or SESIPx with SESIPy part(s))
Certificate Number	SESIP xxxxxxxxxx
Product	
Version	
TOE Type	examples in Table A-2
Sponsor/Vendor	
Security Target Reference	
SESIP Profile Reference & Packages	If no SESIP Profile, state “ST based”
Attacker Profiles	
Certification Type	Composition/Standalone/Dependent
Composition Certificate(s) or Dependency details	Includes certificates from another scheme – or SESIP Cert or Product identifier
Evaluation Lab	
Validity	
CB Specific Information	
Standard, etc.	
Signature, etc.	

A.2 Certificate Associated Taxonomy

Table A-2: Example TOE Types Listed in SESIP Certificates

Term	Definition
Hardware	Hardware module
Firmware	Software module implementing interfaces between software modules and hardware part of the platform
Software standalone	Software module fully independent from the hardware part of the platform
Software dependent	Software module relying on hardware features for some functionality (not necessarily security)
Hard macro	Subcomponent of a hardware module, compiled for integration
Soft macro	Uncompiled hardware library (usually System Verilog)
Microkernel standalone	
Microkernel dependent	
…	

A.3 Certificate QR Code

Each certificate should include a GlobalPlatform SESIP QR Code, which should be directed to the product certification.

There are no special requirements for QR Code production.

Figure A-1: Example of QR Code