GlobalPlatform

PSA Certified Governance

Version 1.0

Release

September 2025

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

1 INTRODUCTION

This document describes the governance framework for PSA Certified. It 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 governance structure is designed to ensure consistency, impartiality, and international recognition of certification outcomes, in accordance with the principles of ISO/IEC 17065.

The use of this document will drive the evolution of the scheme, 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.

The governance process facilitates cooperation between Laboratories and Certification Bodies.

1.1 Audience

This document is intended for all stakeholders involved in PSA Certified activities under GlobalPlatform licensing, including Certification Bodies, Evaluation Laboratories, regulatory authorities, Accreditation Bodies, and organizations relying on peer-assessment. It is also relevant to customers and schemes seeking to confirm or recognize 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]
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]

Standard / Specification	Description	Ref
ISO/IEC 17065:2012	Conformity assessment – Requirements for bodies certifying products, processes and services, September 2012	[ISO 17065]
SESIP	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]
GP_GUI_067	SESIP Governance	[SESIP_GOV]

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 17065], 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
PSA	Platform Security Architecture

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 precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-4: Revision History

Date	Version	Description
July 2025	0.0.0.5	Initial draft
September 2025	1.0	Initial Release

2 DOCUMENT SCOPE

This document defines the governance framework for PSA Certified, a security evaluation scheme for Connected Platforms based on the Platform Security Architecture (PSA). It has been developed using ISO/IEC 17065:2012 as a foundational reference to ensure that the certification process is impartial, consistent, and internationally recognized.

The governance framework outlined here provides supplementary licensing and operational requirements for Certification Bodies and Evaluation Laboratories participating in PSA Certified activities. It is intended to support Accreditation Bodies in harmonizing their assessments of Certification Bodies, and to assist Certification Bodies in aligning their operations with ISO/IEC 17065 requirements.

This document also facilitates:

- Mutual recognition of certification results across jurisdictions.
- Consistency in the application of evaluation methodologies.
- Transparent and traceable certification decisions.
- Cooperation and information exchange between stakeholders.

The requirements for conformity assessment are derived from [ISO 17025] and [ISO 17065].This document does not reproduce the full text of ISO/IEC 17065 or ISO/IEC 17025. Users are expected to obtain these standards from the appropriate standards organizations.

2.1 PSA Certified

PSA Certified is an independent security evaluation scheme for PSA-based IoT systems. It provides a multi-level assurance framework for chips containing a PSA Root of Trust (PSA-RoT), which delivers trusted functionality to the platform.

In August 2025, the PSA Certified scheme was formally transferred to GlobalPlatform, which now maintains and evolves the scheme to ensure its continued relevance and value to the industry.

More information is available at https://www.psacertified.org.

Note: Previous participation in PSA JSA activities may be considered as part of the experience requirements for Certification Bodies and Laboratories, where applicable.

2.2 PSA Certified vs SESIP

The PSA Certified Governance rules are an extension of SESIP Governance ([SESIP_GOV]) and introduces additional requirements specific to PSA Certified. While the two schemes are closely aligned, PSA Certified includes distinct elements such as:

- PSA Certified Level 1
  - PSA Certified level 1 is based on a Certification Body’s review of a laboratory’s assessment of the PSA Certified Level 1 questionnaire, which includes chip, system software, and device assessments
  - The specific process for a Level 1 certification is defined in “PSA Certified™ Level 1 Step-by-Step Guide” currently referenced as JSADEN005 dated “31/03/2021”
- PSA Certified Level 4
  - PSA Certified Level 4 is based on a SESIP Certification with a SESIP protection profile level 3 with a AVA_VAN.4 robustness level

3 CERTIFICATION BODY LICENSING

This section outlines the licensing requirements for Certification Bodies (CBs) participating in the PSA Certified scheme. These requirements are designed to ensure that CBs operate in accordance with ISO/IEC 17065:2012, demonstrating competence, impartiality, and consistency in the certification of products, processes, and services

3.1 Licensing Scope

GlobalPlatform PSA Certified Certification Body licensing will be provided for the entire range of defined PSA Certified assurance levels and profiles.

As the higher range PSA Certified assurance levels and profiles are based on SESIP, the Certification Body must be a GlobalPlatform licensed SESIP Certification Body, ISO17065 accredited and experienced for the highest of the SESIP levels referred to in the PSA Certified assurance levels and profiles.

At the time of writing this governance document, the required level for a Certification Body must be **ISO/IEC 17065 accredited SESIP level 4 with physical attacker**.

3.2 Licensing Requirements

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

- Be a GlobalPlatform SESIP Certification Body with a scope including all PSA Certified assurance levels and profiles (at the time of writing: at least SESIP4 with physical attacker).
- Be a GlobalPlatform “full” or “participating” member
- Be actively participating in the GlobalPlatform SESIP and PSA Certified 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
- Demonstrate technical competence in the SESIP methodology
- Provide proof of expertise in the targeted technical domains and the verification of PSA L1 questionnaires for more than three years
- Demonstrate capacity to assess evaluation laboratories against the targeted technical domains and levels.
- Demonstrate expertise in using rating methodology (example: [AAP]) for technical domains
- Present a yearly report (as discussed in section 3.2.1) to the PSA Certified community

3.2.1 Yearly Report

Every year, each PSA Certified licensed CB shall present to the 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
- PSA Certified evolution proposed following a year of operation

3.2.2 Peer-to-Peer Review

To ensure alignment with PSA Certified certificate values, GlobalPlatform PSA Certified-licensed CBs should participate in regular peer-to-peer reviews as defined by the GlobalPlatform SESIP governance. During peer-to-peer reviews. Licensed CBs must share comprehensive documentation detailing their evaluation and certification scheme processes. Required documentation includes, but is not limited to:

- Annual performance and compliance report
- ISO/IEC 17065 scope of certification activities
- Organizational structure of the certification scheme
- Accreditation and licensing policies for evaluation laboratories, including ISO/IEC 17025 validity and technical domain coverage
- National regulatory frameworks and rules applied to evaluation and certification, where applicable

4 Evaluation laboratory Licensing

This section defines the licensing requirements for Evaluation Laboratories participating in the PSA Certified scheme. These requirements are designed to ensure that laboratories operate in accordance with ISO/IEC 17025 and are assessed by Certification Bodies licensed under ISO/IEC 17065.

4.1 Licensing Scope

GlobalPlatform PSA Certified Evaluation Laboratories will be licensed for defined security assurance level ranges, from PSA Certified L2, based on SESIP level 2 requirements.

Note: PSA Certified Level 1 alone is not eligible for laboratory licensing.

Laboratories must meet the GlobalPlatform governance requirements for the highest SESIP level corresponding to the PSA Certified levels they intend to support.

4.2 Licensing Requirements

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

- Be licensed as a GlobalPlatform SESIP lab
- Be licensed under at least one SESIP CB, for at least the highest SESIP level implied by the highest PSA Certified level
- Be a GlobalPlatform “full” or “participating” member
- Be actively participating in the GlobalPlatform PSA Certified and SESIP standard and interpretations maintenance working groups
- Be actively participating in the GlobalPlatform Attack Expert Working Groups
- For PSA Level 3 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 PSA Certified and SESIP expertise
- Apply the PSA Certified and SESIP methodology

4.3 GlobalPlatform Licensing Process

It is the responsibility of a Global Platform SESIP and PSA Certified licensed Certification Body to ensure that the candidate Laboratory 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 when available.

Annex A SESIP CERTIFICATE

A.1 Publication Process

On completion of the PSA Certification process evaluation, the Certification Body will send the web team an email stating the certification is complete and the publication of the results is possible.

The Email shall contain a completed certificate template as defined in A.2 that should look like this:

Subject: New <L1/L2/L3> certification for <(xxxxxxxxxxxxx)> <TOE Name>

Dear Team

This is a new <L1/L2/L3> certification for <(xxxxxxxxxxxxx)> <TOE Name>

Please find attached:

1. A filled in Certificate Template spreadsheet

2. Webkit information as second tab in spreadsheet

A.2 Certificate Template

Certificate Field	Database ID	Type	Format	Mandatory/Optional	Comments
Certificate Number	id	string	EAN13+5digits	Mandatory	Certificate Number in EAN13+5digits Proposal for EAN13 unique number to be HW version (could be provided by the chip (HW Version) or the certification authority) 5 digits Encoding format: 1st digit (from left): The first digit of the +5 encodes the number of the certification attempts by the lab of this chip type, starting with '1' Remaining 4 digits can be uniquely set by the Certificate Authority or provided by the developers
Certificate Issue Date	certificate_issue_date	string	ISO8601/RFC3339 YYYY-MM-DD Date format	Mandatory	Certificate Issue Date (in ISO8601/RFC3339 YYYY-MM-DD format)
Test Lab	test_lab	string	text	Mandatory	Test Lab Name
Certificate Holder	certificate_holder	string	text	Mandatory	Full Name of the organisation holding the certificate
Certified Product	certified_product	string	text	Mandatory	Certified Product Details
Product Description	product_description	string	text	Mandatory	Description of the certificate
Hardware Version	N/A	string	text	Mandatory	User Readable Hardware Version
Is chip TRNG NIST_SP_800_90B compliant?	entropy_source	string	text	Mandatory for Chip Level	Is TRNG compliant to NIST SP 800-90B? Only for Chip vendors. Needed by Amazon.
Entropy Source	entropy_source	string	text	Mandatory for Chip Level	If the chip's TRNG is compliant to NIST SP 800-90B state it here. If not please state other standard it is compliant to.
SW Information	sw_info	list of dictionaries/structures	sku & name: String Semver: semantic versioning Type: String	Optional	Contains Software Information Software information for Secure Processing Environment
Certificate Standard	certificate_standard	string	text	Mandatory	Standard for which certificate is issued
Certificate Standard Type	certificate_standard_type	string	text	Mandatory	Enum: Chip only, RTOS on uncertified chip, RTOS on certified chip, Device and RTOS on certified chip, Device on certified RTOS and certified chip, Device on uncertified RTOS and uncertified chip

Certificate Field	Database ID	Type	Format	Mandatory/Optional	Comments
Security Level	security_level	Dictionary/ Structure	security level & security level version (Major.Minor)	Mandatory	PSA Security Levels (from below) Level 1 Level 2 RoT Component Level 2 Level 3 iSE/SE Level 2+SE Level 3 RoT Component Level 3 Level 3+SE Level 4 iSE/SE Level 4 RoT Component
Chip Certificate Number		string	text	Mandatory	For composite evaluations
RTOS Certificate Number		string	text	Mandatory	For composite evaluations
UI PSTI section passed?		String	text	Optional	Device level only. Mandatory requirements met, minimum information for statement of compliance met, or rationale of why N/A.
EU Cyber Resilience Act section passed?		string	text	Optional	Chip, System Software and Device applicability. Essential Requirements met (7.22, 7.23 & 7.24) or rationale provided of why N/A
RED Cybersecurity section passed?		string	text	Optional	Device level only. Mandatory requirements met, minimum information for statement of compliance met, or rationale of why N/A.
ETSI 303 645 v2 mappings complete?		string	text	Optional	
NIST 8259 draft v2 mappings complete?		string	text	Optional	
SB-327 (CA IoT law) mapping complete?		string	text	Optional	
DCMS draft IoT requirements - mapping complete?		string	text	Optional	
	Link to the developer's website for the product				
	Whether the developer would like to use the PSA Certified logo and trademarks				