GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
SE Certification Process
Version 2.0

Public Release

January 2021

Document Reference: GP_PRO_048

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

1.1 Scope

This document describes the processes and requirements associated with the GlobalPlatform SE Security Scheme for the certification of security evaluations of Products and the accreditation of SE evaluation laboratories. GlobalPlatform Certification Body is the entity that operates the scheme and is responsible for enforcing the GlobalPlatform **SE Certification Process**, as defined in this document.

The GlobalPlatform website (today at https://globalplatform.org/certifications/) provides the latest requirements documents including Protection Profiles, Operation Bulletins, the list of Accredited Laboratories, and the certification fee policy. In any case of difference in contents, the versions of the documents published on the website apply and supersede the information that is provided in this document.

This document is organized as follows:

- Chapter 1 defines the terminology and provides the list of applicable references.
- Chapter 2 presents the principles of the scheme.
- Chapter 3 presents the product evaluation and certification processes.
- Chapter 4 presents the laboratory accreditation requirements and related processes.

1.2 Audience

This document is intended primarily for SE developers and manufacturers, collectively referred to as Product Vendors, and for laboratories performing SE and eUICC security evaluations.

This document is also intended for the users of SE or eUICC products, such as mobile network operators, service providers, and OEMs.

1.3 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.

1.4 References

The following references are relevant to the SE Certification Process. Unless stated otherwise, the latest official release applies. GlobalPlatform documents listed below are accessible from either the public or the member GlobalPlatform website portal.

Table 1-1: Normative References

Standard / Specification	Description	Ref
	Joint Interpretation Library – Application of Attack Potential to Smartcards, version 3.1, June 2020	[JIL-AAPS]
	Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, version 2.2, January 2013	[JIL-AMSC]
BSI-CC-PP-0035-2017	Security IC Platform Protection Profile	[PP-0035]
BSI-CC-PP-0084-2014	Security IC Platform - Protection Profile with Augmentation Packages	[PP-0084]
Common Criteria	Common Criteria for Information Technology Security Evaluation: – Part 1: Introduction and general model, April 2017, version 3.1, revision 5, reference CCMB-2017-04-001 – Part 2: Security functional components, April 2017, version 3.1, revision 5, reference CCMB-2017-04-002 – Part 3: Security assurance components, April 2017, version 3.1, revision 5, reference CCMB-2017-04-003	[CC]
Common Evaluation Methodology	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, April 2017, version 3.1, revision 5, reference CCMB-2017-04-004	[CEM]
GP_AGR_201	GlobalPlatform SE Security Evaluation Agreement Exhibit B – GlobalPlatform SE Product Evaluation Request Form Public	[SE A]
GP_AGR_202	GlobalPlatform Laboratory Accreditation Request Form Public	[LAB R]
GP_AGR_204	GlobalPlatform SE Security Laboratory Relationship Agreement Public	[LAB A]
GPC_GUI_163	GlobalPlatform SE/eUICC Evaluation Methodology Member *Available by request to non-member Product Vendors.*	[SE EM]
GPC_SPE_174	GlobalPlatform SE Protection Profile (and SE PP-Modules) Public Remark: This reference stands for the SE PP and all applicable PP-Modules for a given Product.	[SE PP]
GPC_TEN_166	GlobalPlatform SE/eUICC Security Target Template	[SE ST]
ISO/IEC 17025:2017	General requirements for the competence of testing and calibration laboratories	[ISO 17025]
SGP.05	Embedded UICC Protection Profile v1.1 (BSI-CC-PP-0089-2015)	[SGP.05]

Standard / Specification	Description	Ref
SGP.16	M2M Compliance Process v1.2, November 2019	[SGP.16]
SGP.24	RSP Compliance Process v2.2, September 2019	[SGP.24]
SGP.25	Embedded UICC for Consumer Devices Protection Profile v1.0 (BSI-CC-PP-0100-2018)	[SGP.25]

1.5 Terminology and Definitions

Selected terms used in this document are included in Table 1-2.

Table 1-2: Terminology and Definitions

Term	Definition
Application Form	See *Product Evaluation Request Form*.
Certificate	A written statement that documents the decision of GlobalPlatform CB that a specified Product has demonstrated sufficient conformance to the GlobalPlatform security requirements as of its evaluation date.
Certification Body (CB)	See *GlobalPlatform Certification Body*.
Certification Report	A document issued by GlobalPlatform CB that summarizes the results of a Product evaluation and confirms the overall results, i.e. that the evaluation has been properly carried out, that the GlobalPlatform Evaluation Methodology has been correctly applied, and that the conclusions of the *Evaluation Technical Report* are consistent with the adduced evidence.
GlobalPlatform Accredited Security Laboratory	A laboratory or test facility that has been accredited by GlobalPlatform to perform SE security evaluations.
GlobalPlatform Auditor	Personnel of GlobalPlatform CB performing accreditation audits of security evaluation laboratories.
GlobalPlatform Certification Body (GlobalPlatform CB)	The GlobalPlatform entity that manages all GlobalPlatform certification schemes.
GlobalPlatform Security Laboratory Relationship Agreement	Agreement between GlobalPlatform and the accredited laboratory ([LAB A]).
Product	An SE or embedded UICC Product submitted for security evaluation and certification.
Product Evaluation Request Form	A completed written request for security evaluation of a Product by a Product Vendor ([SE A])
Product Registration Number	A unique number identifying the Product, assigned by GlobalPlatform CB at the start of the certification process.
Product User	Any actor that relies on SE security features as stated in PPs.
Product Vendor	An entity submitting a Product for assessment under the Certification Process, which acts as sponsor of the evaluation and certification.

Term	Definition
Restricted Certificate	The written recognition and acknowledgement of restricted certification of a Product, provided by GlobalPlatform CB to a Product Vendor for a Product that is found to have some residual vulnerabilities under the evaluation and certification process.
Restricted Certification Report	A *Certification Report* based on an *Evaluation Technical Report* that identifies residual vulnerabilities.
Risk Analysis Report	The report, prepared jointly by GlobalPlatform CB and the Product Vendor in the event the Product Vendor decides not to remedy the Product vulnerabilities identified as part of the evaluation and certification process, and containing information for third parties intending to use the Product.
Security Certificate Number	A unique reference number that applies exclusively to the exact Product configuration described in the GlobalPlatform Certificate.
Security Requirements	Collectively, the most recent version (unless GlobalPlatform specifies an earlier version) of the applicable PPs and PP-Modules, SE/eUICC Evaluation Methodology, JIL Attack Catalog, and all amendments, modifications, and upgrades as adopted by GlobalPlatform from time to time.

1.6 Abbreviations and Notations

The abbreviations and notations listed in Table 1-3 apply.

Table 1-3: Abbreviations and Notations

Abbreviation / Notation	Meaning
CB	Certification Body
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
eUICC	Embedded UICC
IAR	Impact Analysis Report
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
PPs	All Protection Profiles supported by the SE scheme
PTP	Penetration Test Plan
SE	Secure Element
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation

1.7 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
March 2019	1.0	First published version
January 2021	2.0	Public Release Alignment with GlobalPlatform CB Quality Manual and current versions of SE Protection Profile and Evaluation Methodology

2 Principles of SE Security Scheme

2.1 Processes and Actors

2.1.1 General

The GlobalPlatform SE Security Scheme embodies the following four main processes:

- Definition and maintenance of **SE Security Requirements**, performed by GlobalPlatform Certification Body and GlobalPlatform technical working groups
- Laboratory accreditation, performed by GlobalPlatform Certification Body and GlobalPlatform Auditors
- Evaluation of Products, performed by GlobalPlatform Accredited Security Laboratories with the support of Product Vendors, monitored by GlobalPlatform Certification Body
- Certification of TEE Products' evaluation, performed by GlobalPlatform Certification Body

The following sections describe the role of the actors involved in the SE Security Scheme.

2.1.2 GlobalPlatform Certification Body

GlobalPlatform is the owner of the GlobalPlatform SE Security Scheme for the certification of security evaluations of Products and the accreditation of SE evaluation laboratories.

GlobalPlatform Certification Body (CB) is the entity that operates the scheme and is responsible for enforcing the GlobalPlatform **SE Certification Process**.

GlobalPlatform CB is in charge of:

- Definition and maintenance of the **SE Certification Process** (this document)
- Definition and maintenance of the **SE Security Requirements** (see section 2.2)
- Laboratory accreditation and management (see Chapter 4)
- Product Vendor evaluation request validation and evaluation monitoring (see Chapter 3)
- Certificate issuance, publication, and management (see section 3.5)

More precisely, the role of GlobalPlatform CB in the evaluation and certification processes (see Chapter 3) consists of the following activities:

- Provide the **Security Evaluation Agreement** to the Vendor.
- Review and validate the **Product Evaluation Request Form** (also called **Application Form**) and companion documentation and provide a registration reference.
- Review and validate the **Penetration Test Plan** and companion documentation.
- Review and validate the **Evaluation Technical Reports (ETR and ETR-Lite)**.
- Establish the **Risk Analysis Report** with the Product Vendor (if applicable).
- Write a **(Restricted) Certificate**.
- Issue the **(Restricted) Certification Report** upon successful evaluation of the Product.
- Publish certificates on the SE Security Scheme webpage unless otherwise decided by the Product Vendor.

Vendors can contact GlobalPlatform CB at certification@globalplatform.org or any other contact address provided on GlobalPlatform's website.

2.1.3 GlobalPlatform Auditors

GlobalPlatform Auditors are personnel of the Certification Body performing the accreditation audits of security evaluation laboratories.

More precisely, the role of GlobalPlatform Auditors consists of reviewing and validating the documentation provided by the laboratory to demonstrate the compliance with the Laboratory Accreditation Requirements defined in section 4.2.

2.1.4 GlobalPlatform Accredited Security Laboratories

GlobalPlatform Accredited Security Laboratories for the evaluation of Products must comply with the criteria set out in section 4.2 of this document, which requires being a “Qualified EAL1-EAL7 for Smartcards and similar devices” by the SOG-IS organization.

GlobalPlatform Accredited Security Laboratories must be members of GlobalPlatform and must contribute to the definition and maintenance of the scheme requirements and processes through their participation in the scheme’s technical working groups.

The relationship between GlobalPlatform and its Accredited Laboratories is enforced by the **GlobalPlatform Security Laboratory Relationship Agreement**, which describes the obligations of the laboratory in terms of structure, skills, and management of the evaluations during the accreditation period.

GlobalPlatform Accredited Security Laboratories are responsible for:

- Renewing their accreditation every two years;
- Informing GlobalPlatform CB in case of change of some of the accreditation conditions, e.g. changes to the expert staff, ownership or management structure, legal status, locations, or third-party accreditations;
- Evaluating Products against the **SE Security Requirements** using the SE/eUICC Evaluation Methodology ([SE EM]);
- Writing the **Evaluation Technical Report (ETR)** and extracting the **ETR-Lite** if applicable.

2.1.5 Product Vendors

Product Vendors request the security evaluation of their Products to GlobalPlatform CB and provide all the necessary materials to the laboratory.

Product Vendors are responsible for:

- Contracting with a GlobalPlatform Accredited Security Laboratory;
- Providing a complete **Product Evaluation Request Form** and selecting the evaluation type (Full, Delta, Fast-track, or Reassessment);
- Providing the **Security Target** of their Product compliant with the applicable Protection Profile, e.g. GlobalPlatform SE Protection Profile;
- Providing the **Impact Analysis Report** of their Product, if applicable;
- Providing the additional information and material listed in [SE EM] to the GlobalPlatform Accredited Security Laboratory;
- Communicating about any previous evaluation or certification of the Product.

The relationship between GlobalPlatform and the Product Vendors is enforced by the Security Evaluation Agreement that describes the mutual obligations.

The selection of the GlobalPlatform Accredited Security Laboratory and the contractual terms of the evaluation are out of scope of GlobalPlatform SE Security Scheme.

2.1.6 Product Users

A Product User is any actor that relies on SE security features as stated in PPs; for instance, a digital service provider or a device integrator (OEM).

When relying on a certified Product, the Product User is responsible for checking the **Certificate** and the corresponding **Certification Report**, in particular:

- The type of the **Certificate (unrestricted or restricted)**
- The scope of the certification, i.e. the security features of the Product that have been evaluated and are covered by the **Certificate**
- The assumptions about the operational environment where the Product is to be used or integrated
- The limitations in case of a **Restricted Certificate**

2.2 SE Security Requirements

2.2.1 General

The SE Security Scheme is built on a set of specifications called **SE Security Requirements** which contains:

- This document
- [SE EM], which relies on JIL attack methods documentation [JIL-AAPS] and [JIL-AMSC]
- The Protection Profiles applicable to GlobalPlatform Card Technology-based products with IC certified at EAL4+ or higher, such as:
  - The GlobalPlatform SE Protection Profile ([SE PP])
  - The GSMA Embedded UICC Protection Profile ([SGP.05])
  - The GSMA Embedded UICC for Consumer Devices Protection Profile ([SGP.25])

These documents are defined and maintained by the technical security working groups of their owners, which ensure high standard developments that meet both market requirements and the state-of-the-art.

Such collaboration between all the stakeholders is key to the acceptance and recognition of the SE Certification Process.

GlobalPlatform Certification Body manages all questions regarding the application of **SE Security Requirements** through the address certification@globalplatform.org.

The following sections describe the owner, content, audience, and distribution of the **SE Security Requirements**.

2.2.2 Certification Process Document

Owner: GlobalPlatform CB.

Content: SE Security Certification process and Laboratory Accreditation requirements and process.

Audience: Laboratories, Product Vendors, Product Users.

Distribution: The latest document is available on the public website www.globalplatform.org.

2.2.3 Protection Profiles

Owner: GlobalPlatform SE Security Working Group for [SE PP], GSMA for [SGP.05] and [SGP.25]; potentially other organizations for certified Protection Profile based on GlobalPlatform Card technology.

Content: Each PP is defined as per the Common Criteria (CC) rules ([CC]). They define the Target of Evaluation (TOE) and its assets, the threat model, the assumptions, the security objectives, the Security Functional Requirements (SFRs), and the evaluation assurance level EAL4+, which consists of EAL4 as defined in [CEM] augmented with ALC_DVS.2 and AVA_VAN.5.

Updates may be triggered by:

- Additional features in the SE specifications
- Specification update with an impact on security
- New attacks or attack techniques, especially those included in revisions of [JIL-AMSC] and [JIL-AAPS]

The update can give rise to the modification of the existing PP or to the creation of new PP-Modules.

Protection Profile Certification: Each Protection Profile has been certified by a Common Criteria scheme and is recognized under CCRA and SOG-IS MRA.

Audience: Laboratories, Product Vendors, Product Users.

Distribution: The applicable Protection Profiles and PP-Modules are available on the public website www.globalplatform.org and on the Common Criteria portal https://www.commoncriteriaportal.org.

2.2.4 Evaluation Methodology

Owner: GlobalPlatform SE Security Working Group.

Content: [SE EM] describes the process and requirements for Vendors and GlobalPlatform Accredited Security Laboratories to perform SE evaluations conformant with the Security Functional Requirements and assurance level defined in the PPs. Security testing relies on the attack methods developed by JHAS working group. [SE EM] is based on EAL4+ evaluation methodology as defined in [CEM], [JIL-AAPS], and [JIL-AMSC].

Updates to [SE EM] may be triggered by:

- Feedback from the field
- Modification of the scope, acceptable form-factors, automated test list, etc.
- Reuse of results from other evaluation schemes
- GlobalPlatform or GSMA specification update
- Attack methods update [JIL-AAPS], [JIL-AMSC]
- Protection Profile update

Audience: Laboratories and Product Vendors.

Distribution: [SE EM] is available to GlobalPlatform Members through the member website https://members.globalplatform.org and to interested Product Vendors upon request to GlobalPlatform CB.

2.2.5 Attack Methods

Owner: JIL Working Group

Content: The documents [JIL-AMSC] and [JIL-AAPS] illustrate the set of attacks that must be considered in an SE evaluation.

Updates of the Attack Catalog may be triggered by:

- New attacks in the field or new attack techniques
- Protection Profile scope evolution

Audience: Laboratories and Product Vendors.

Distribution: The distribution of these documents is restricted to laboratories that are qualified for smartcards and similar devices evaluation by a SOG-IS certification scheme.

2.3 Target of Evaluation

The TOE is an SE or eUICC which is developed on an IC certified according to [PP-0084] or [PP-0035] by a SOG-IS scheme.

The TOE comprises the hardware, firmware, and software components and mechanisms that provide the security features as defined in the applicable PPs and PP-Modules.

Technically, the TOE is the part of the Product that is in the scope of the vulnerability analysis and testing as defined in [SE EM]. However, for the sake of simplicity *TOE* and *Product* are used interchangeably in this document.

2.4 Security Evaluation

2.4.1 General

The GlobalPlatform SE Certification Process requires an independent evaluation of the Product against the requirements of an allowed Protection Profile and the support of the Product Vendor to provide accurate and up-to-date information and materials to the GlobalPlatform Accredited Security Laboratory in charge of the evaluation.

The Evaluation Methodology described in [SE EM] seeks to optimize the cost and time of the evaluation activities. By leveraging Full, Delta, Fast-track, and Reassessment evaluations, Products can be evaluated and certified in an incremental approach where the design is evaluated once and the paperwork overhead is reduced. The document [SE EM] defines the inputs required from the Product Vendor and the analysis and testing steps that the laboratory must perform to assess the security mechanisms of the Product. The laboratory carries out an independent vulnerability analysis that allows to derive a specific set of relevant penetration tests based on the Product characteristics.

2.4.2 Types of Evaluations

GlobalPlatform SE Security Certification scheme relies on four types of evaluations:

- Full evaluation: It applies to Products that have not been evaluated before or that have been significantly changed since the previous evaluation. A Full evaluation includes all the Security Requirements stated in the applicable Protection Profile and the selected PP-Modules.
- Delta evaluation: It applies to a TOE that is an updated version of a certified TOE (original TOE) with valid certificate. The Vendor must provide an **Impact Analysis Report** (IAR) describing all the product changes and their security impact to the laboratory, which then issues a recommendation with regard to the type of evaluation that should be performed. The Vendor then submits the IAR and the recommendation statement to GlobalPlatform CB, which decides about the possibility to apply a Delta evaluation process.
- Fast-track evaluation: It can be used for changes to a certified TOE (original TOE) with valid certificate that do not impact its security. The Vendor must provide an **IAR** describing all the product changes and a rationale demonstrating the absence of security impact to GlobalPlatform CB which decides on the application of the Fast-track evaluation process. The principle is that any security change in the product gives rise to a Full or a Delta evaluation.
- Reassessment: It can be used to renew the certificate of a certified TOE, if the IC certificate is still valid on the basis of up-to-date **SE Security Requirements**.

The Product Vendor shall refer to [SE EM] for a complete description of the evaluation types.

2.4.3 Reuse of Evaluation Work

GlobalPlatform allows reusing evaluation results through Delta, Fast-track, and Reassessment evaluation processes. Moreover, GlobalPlatform may allow reusing certification or evaluation results completed prior to the application for certification in the GlobalPlatform SE scheme upon vendor request. GlobalPlatform reserves the right to accept or deny such reuse. The decision is performed on a case-by-case basis.

The prior certification and/or evaluation must be unambiguously identified in the **Product Evaluation Request Form**.

2.5 Security Certification

2.5.1 General

The output of a successful evaluation in the GlobalPlatform SE Security Scheme is a GlobalPlatform **Certificate**.

In case potential vulnerabilities are found during the evaluation, GlobalPlatform may either deny to certify the Product or issue a **Restricted Certificate**. If this happens, the Product Vendor is informed of the details and GlobalPlatform works with the Vendor to ensure that:

- The vulnerabilities are adequately communicated by the Product Vendor to the SE scheme users to enable appropriate risk management;
- A plan is put in place by the Product Vendor to release a revised Product that reduces or removes the vulnerabilities.

GlobalPlatform reserves the right to withdraw or not issue a **(Restricted) Certificate** when there is no sufficient evidence that the Product can resist to the attack potential as defined in PPs or when potentially exploitable vulnerabilities have been identified.

Each certificate has a unique **Security Certificate Number** that applies to the exact Product configuration(s) described in the certificate.

Certified Products are listed in the GlobalPlatform Certified Products List. A Product is removed from the list upon expiration or withdrawing of the certificate.

2.5.2 Recognition of Common Criteria Certificates

GlobalPlatform has defined the conditions under which CC certificates of Products issued by a CC certification body could be recognized:

1. The CC certification body is participating in the SOG-IS organization.
2. The Security Target of the CC certified product claims conformance with a valid version of the applicable Protection Profile at the date of certification.
3. The Security Target claims conformance with the assurance components of the Evaluation Assurance Level defined in the PP.
4. The evaluation of the Product has been made using a valid version of the JIL documents [JIL-AMSC] and [JIL-AAPS].
5. The CC evaluation has been performed by a laboratory that is “Qualified EAL1-EAL7 for Smartcards and similar devices” by the SOG-IS organization.
6. GlobalPlatform CB is informed of the issuance of the CC Certificate within ten (10) days from the issuance of the Certificate.
7. GlobalPlatform CB receives the Security Target and the CC Certification Report within ten (10) days from the issuance of the Certificate.
8. The CC certification body supports GlobalPlatform CB risk management activities related to potential vulnerabilities of the CC-certified Product, in the event of new attacks in the field or new attack methods.

2.5.3 Risk Management

Product Users are in a risk management business that requires constant monitoring of vulnerabilities and threats. The Vendor that sells a certified Product should be able to explain the testing that has been carried out in order to verify the conformance with GlobalPlatform **SE Security Requirements**.

The level of testing reflects the attacks’ state-of-the-art at the time of certification. However, testing cannot anticipate all future attacks. Consequently, the introduction of new products should offer enhanced protection against the latest threats.

Product Users should constantly bear in mind that there is no perfect security and that the security level of a given Product is likely to decrease over time. An attack made with sufficient resources in terms of skills, equipment, and time is likely to succeed in compromising the Product’s assets. A secure system must implement defenses at all levels, and Product Users should develop strategies of attack prevention, detection, and recovery. Incident management procedures should be in place and appropriate measures should be taken to limit the likely benefits that an attacker may achieve. The GlobalPlatform SE Certification Process aims at providing an independent statement about the resistance level and the potential vulnerabilities of the Product, which can be integrated into the User’s risk analysis.

In the event that a Product only receives a GlobalPlatform **Restricted Certificate**, the Product Vendor should be in a position to explain the reasons, and to offer guidance about the potential risks to the implementation plans of Product Users. Product Users may mitigate these risks – to a level that is acceptable to them – by using complementary security measures.

2.6 Language

The official language of the SE Security Scheme is English. The use of any other language is subject to GlobalPlatform approval.

3 Product Evaluation and Certification

3.1 Full Evaluation

3.1.1 Application

3.1.1.1 Product Evaluation Request

In the framework of a Full evaluation, the Product Vendor shall submit to GlobalPlatform CB the **Product Evaluation Request Form (or Application Form)**, containing the product identification details and the laboratory name, together with the Security Target and the list of evidences of previous independent security evaluations/certifications carried out on the product.

The Product Vendor shall declare in the **Product Evaluation Request Form** whether the Product and the project are confidential, and whether the **Certificate** is expected to be published on GlobalPlatform's website or not. The publication choice may be modified at the end of the certification process.

GlobalPlatform CB provides its public key to protect the product-related documentation that is required from the vendor and from the laboratory during the entire certification project.

3.1.1.2 Application Review

GlobalPlatform CB examines the evaluation request and the related documents and notifies the vendor about the decision: acceptance, denial, or request for complementary information or update of the documents.

Upon acceptance, GlobalPlatform and the Product Vendor sign the **GlobalPlatform Security Evaluation Agreement**. GlobalPlatform CB then registers the certification request and provides a unique **Product Registration Number** for use in all communications up to the certification decision.

3.1.2 Evaluation

3.1.2.1 Evaluation Start

The Product Vendor shall contract with a GlobalPlatform Accredited Security Laboratory to perform the evaluation of its Product. The contractual phase and the terms of the contract are out of scope of the GlobalPlatform SE scheme.

In order to start the evaluation, the laboratory must provide the evaluation workplan to GlobalPlatform CB with the identification of the evaluation team, the effort expected for each evaluation activity as defined in [SE EM], and the schedule. The evaluation can officially start only if the following conditions are met:

- **GlobalPlatform Security Evaluation Agreement** has been signed by both parties, which requires the approval of the **Product Evaluation Request Form** and the **Security Target**;
- GlobalPlatform CB has approved the evaluation workplan;
- The laboratory has received from the Vendor all the inputs that are necessary to perform the evaluation as defined in [SE EM].

GlobalPlatform CB organizes a kick-off meeting with the laboratory and the vendor and approves the actual evaluation workplan including the project schedule.

3.1.2.2 Product Assessment

The laboratory shall perform the Product evaluation against the requirements covered by the scope of certification in compliance with [SE EM], i.e. the evaluation consists of a vulnerability analysis phase (documentation review, source code inspection, and possibly some manual and/or automated testing) which gives rise to a Penetration Test Plan submitted to GlobalPlatform CB, and a functional and penetration testing phase of the security functionality that addresses the behavior of the security functionality and covers the attack methods described in JIL documents [JIL-AMSC] and [JIL-AAPS].

GlobalPlatform CB reviews the Penetration Test Plan (PTP) and confirms that the PTP is adapted to the ST and fully answers to the targeted security for the scheme.

The typical duration of a GlobalPlatform SE evaluation is less than three (3) months, provided the Product complies with GlobalPlatform and/or GSMA specifications and all the necessary evaluation inputs are available as required in [SE EM], e.g. Security Target, source code, samples. Such a duration applies for one product version.

Nevertheless, there is no formal obligation in general to perform the evaluation in less than three (3) months. More time might be necessary where, for instance, the product requires security updates or either the laboratory or GlobalPlatform CB considers that additional analysis and/or testing is necessary. However, vendor and laboratory are expected not to delay the evaluation project unduly and to make their best efforts to perform the Product assessment in a reasonable timeframe. The default maximum duration of a certification project is nine (9) months from the registration date. GlobalPlatform CB, at its own discretion and under special circumstances, may extend such period.

GlobalPlatform CB monitors the evaluation progress as defined in [SE EM], including the review and validation of the Penetration Test Plan. The laboratory shall inform GlobalPlatform CB of all identified nonconformities at least at every monitoring point.

GlobalPlatform CB informs the vendor of all nonconformities raised by the laboratory or identified by the CB.

GlobalPlatform CB, in coordination with the laboratory, provides information regarding the additional evaluation tasks needed to verify that nonconformities have been corrected. If the Vendor agrees to continue with the certification process, the additional evaluation tasks are integrated into the evaluation plan and the evaluation resumes under an updated evaluation workplan subject to approval by GlobalPlatform CB.

3.1.2.3 Evaluation Reports

After evaluation, the GlobalPlatform Accredited Security Laboratory shall issue the **ETR** and optionally the **ETR-Lite** as defined in [SE EM]. **ETR** and **ETR-Lite** shall contain the description and outcomes of the vulnerability analysis and testing as well as:

- The laboratory’s verdict with regard to the Product’s resistance to attackers with attack potential as defined in the applicable Protection Profile, provided the use of the Product complies with its security guidance;
- All the vulnerabilities that have been identified and might be exploitable within the operational environment and attack potential defined in the applicable Protection Profile, which is covered by dedicated recommendations given in the Product’s security user guidance;
- All the residual vulnerabilities that have been discovered and might be exploitable outside the conditions of the evaluation, i.e. either in an operational environment that does not comply with the applicable Protection Profile or with an attack potential that goes beyond the requirements and does not comply with the threshold defined in the applicable Protection Profile.

The **ETR** and **ETR-Lite** are transmitted to the Vendor and to GlobalPlatform CB. The **ETR-Lite** contains a subset of the information presented in the **ETR** and is expected to be shared with third parties on a need-by-need basis.

3.1.2.4 Evaluation Review

GlobalPlatform CB reviews the Penetration Test Plan and the **ETR** and determines if the evaluation results provide sufficient assurance that the Product and the evaluation work comply with the **SE Security Requirements**. Based on all the information gathered from the evaluation, the reviewer makes a recommendation for a certification decision. The evaluation review may give rise to the request for additional information and/or complementary evaluation activities.

3.1.3 Certification

3.1.3.1 Certification Decision

GlobalPlatform CB makes the certification decision based on all the information related to the evaluation and the recommendation of the reviewer(s).

In case of a decision to certify the product, GlobalPlatform CB writes the **Certification Report**.

In case of a decision not to certify the product, GlobalPlatform CB notifies the vendor and identifies the reasons for the decision. Should GlobalPlatform CB consider that the evaluation process can be resumed and the vendor express interest in continuing the certification process, this is dealt with as described in section 3.1.2.2.

3.1.3.2 Certification Report and Certificate

In case of a decision to certify the product, GlobalPlatform CB writes the following two documents as defined in section 3.5.1:

- **Certification Report** – Shall be communicated to the vendor and the laboratory for review prior to official release.
- **Certificate** – Shall be signed by a GlobalPlatform authorized representative.

The **Certificate** shall contain a unique **Security Certificate Number**.

The issuance of the certification documentation requires that the Vendor Agreement is signed and all administrative and financial conditions are fulfilled.

3.1.4 Risk Analysis Report

Under some circumstances, based on the evaluation results and the reviewer(s) recommendation, the Product Vendor and GlobalPlatform CB may decide together to perform an assessment of the risks resulting from nonconformities or residual vulnerabilities that have been identified and that are considered significant by GlobalPlatform or by the Vendor. Following such analysis, two situations may arise:

1. GlobalPlatform proposes to issue a **Restricted Certificate**, which requires the agreement of the Vendor to prepare a joint **Risk Analysis Report** containing information for Product Users;
2. GlobalPlatform declines to certify the product “as is”. The product vendor may decide to remedy such residual vulnerabilities and re-start the certification process.

Where the decision is to prepare a **Risk Analysis Report**, GlobalPlatform reserves its final authority over its content to ensure that Product Users receive reliable information derived from the SE evaluation, which is meaningful to the risk assessment of their SE services or deployments.

GlobalPlatform CB then writes the following documents:

- **Restricted Certification Report**, including a reference to the **Risk Analysis Report**
    - GlobalPlatform CB transmits the Restricted Certification Report to the laboratory and to the vendor for review prior to official release.
- **Restricted Certificate,** which shall be signed by a GlobalPlatform authorized representative

The issuance of the restricted certification documentation requires that the Vendor Agreement is signed and all administrative and financial conditions are fulfilled.

3.1.5 Product Identification

The following requirements apply to the identification of the Product from the initial request up to the certification. Product code-name is allowed temporarily; real Product version and TOE components identification data are always required.

Upon evaluation request:

- Product name and version are required in the **Product Evaluation Request Form** for registering a SE evaluation:
    - Product code-name can be used at request time.
    - The Product version must match the real version in Vendor's systems.
- Product name and version as well as identification of TOE components are required in the Security Target (see GlobalPlatform SE Security Target Template – [SE ST]):
    - The same name and version used in the request form can be used in the Security Target for application review.
    - The identification of the TOE and TOE components must match the real unique identification data (e.g. name and version) in Vendor's systems. This applies to the identification of the IC, the platform, and preloaded applications.

During evaluation:

- The laboratory must be able to identify the TOE and TOE components and must keep track of all the versions used in the security assessment.
- The laboratory must be able to identify the testing material, e.g. samples, source code, and must keep track of all the versions used in the security assessment.
- The Vendor must be able to recover from their configuration management system the initial version(s) of the TOE and TOE components and all the versions transmitted or made accessible to the laboratory.
- The Vendor must be able to recover from their systems the configuration of all the versions of the testing material that have been provided or made accessible to the laboratory.

At evaluation reporting time:

- The final Security Target must include the real Product name and version.
- The final Security Target must include the real identification of the TOE and TOE's components, as evaluated by the laboratory.
- The **ETR** and **ETR-Lite** must provide the real Product name and version, as per the final Security Target.

- The **ETR** and **ETR-Lite** must identify all the versions of the TOE and TOE's components that have been audited/tested during the evaluation.
- The **ETR** and **ETR-Lite** must identify the final versions of the TOE and TOE components upon which the evaluation verdict has been made, as per the final Security Target.

At certification time:

- The **(Restricted) Certification Report** and corresponding **(Restricted) Certificate** shall include the real Product and TOE components identification, as per the final Security Target, the **ETR**, and the **ETR-Lite**.
- The **(Restricted) Certification Report** and corresponding **(Restricted) Certificate** may include the commercial Product name upon Vendor's request.

3.2 Delta Evaluation

In order to apply for a Delta evaluation of a new Product, the Vendor prepares an **Impact Analysis Report** (IAR) describing all the hardware and software changes to the original certified Product and their security impact and submits the IAR to the selected laboratory for review. The laboratory assesses the feasibility of the Delta evaluation and issues a recommendation. Both the IAR and the laboratory's recommendation are provided to GlobalPlatform CB together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform CB then examines the Delta evaluation request and notifies the Vendor about the decision: acceptance, denial, or request for complementary information.

The Delta evaluation steps are the same as in a Full evaluation. Upon successful evaluation, GlobalPlatform issues a **Derived Certificate** for the new Product, which references the original **Certificate**.

3.3 Fast-track Evaluation

In order to apply for a Fast-track evaluation of a new Product, the Vendor prepares an **Impact Analysis Report** (IAR) describing all the hardware and software changes to the original certified Product and containing a rationale that shows that the changes do not impact the security of the Product. The IAR is provided to GlobalPlatform CB together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform CB then examines the Fast-track evaluation request and notifies the Vendor about the decision: acceptance, denial, or request for complementary information.

Upon acceptance of Fast-track evaluation, GlobalPlatform performs all the technical and administrative steps to issue the **Derived Certificate** of the new Product, which shall reference the original **Certificate**.

Fast-track evaluation does not involve testing activities by a laboratory.

3.4 Reassessment Evaluation

In order to apply for a Reassessment evaluation of a Product, the Vendor prepares an **Impact Analysis Report** (IAR) describing the status of the IC certificate and potential hardware and software changes to the original certified Product and containing a rationale that shows that the changes do not impact the security of the Product. The IAR is provided to GlobalPlatform CB together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform CB then examines the Reassessment evaluation request and notifies the Vendor about the decision: acceptance, denial, or request for complementary information.

Upon acceptance of Reassessment evaluation, GlobalPlatform performs all the technical and administrative steps (same as in a Delta evaluation) to renew the **Certificate** of the Product, with an extended expiry date.

3.5 Certificate Management

3.5.1 Certificate

A GlobalPlatform **Certificate** confirms that the Product identified in the certificate has undergone security evaluation by an Accredited Laboratory against a PPs-conformant ST as defined in [SE EM], and that no significant residual vulnerability has been identified. It includes:

- Security Certificate Number
- Issuance date
- Identification of the TOE
- TOE type
- Identification of the Sponsor (the Vendor)
- Identification of the developer(s)
- Protection Profile conformance claim
- Identification of the Accredited Laboratory that performed the evaluation
- Evaluation type (Full, Delta, Fast-track, or Reassessment)
- Certification type (full or restricted)
- Reference of the **Certification Report**

For a Delta or Fast-track evaluation, the reference to the original **Certificate** is included.

A GlobalPlatform **Certification Report** includes:

- Certification Report number
- Certification Report issuance date
- Product Registration Number
- All the information contained in the **Certificate**
- Identification of the TOE documentation including the Security Target and the User Guidance
- Identification of the Evaluation Methodology and attack methods documents used during the evaluation
- Evaluation scope (description of the TOE functionalities that have been tested)
- Summary of the evaluation activities
- Assumptions and usage restrictions (if applicable)
- Conclusion

For a Delta, Fast-track, or Reassessment evaluation, the reference to the original **Certificate** and **Certification Report** are included.

For a Fast-track evaluation, the chapters about evaluation scope and activities are empty.

3.5.2 Restricted Certificate

A GlobalPlatform **Restricted Certificate** confirms that the product identified in the **Certificate** has undergone security evaluation by an Accredited Laboratory against the applicable Protection Profile requirements as defined in SE_EM, and that the laboratory has discovered some significant residual vulnerabilities which have been addressed in a specific **Risk Analysis Report**.

A GlobalPlatform **Restricted Certificate** includes all information contained in an unrestricted certificate as defined in section 3.5.1 and the reference of the correspondent **Restricted Certification Report**.

A GlobalPlatform **Restricted Certification Report** includes all information contained in an unrestricted certification report as defined in section 3.5.1 and the reference of the correspondent **Risk Analysis Report.**

3.5.3 Certification Validity

By default, a GlobalPlatform **(Restricted) Certificate** issued from a Full evaluation is valid for five (5) years from the certification date.

A successful Delta or Fast-track evaluation give rise to a **Derived Certificate** with the same validity date of the original **Certificate**.

A successful Reassessment evaluation gives rise to a **Certificate** with an extended validity date as compared to the original **Certificate**. Note: The Vendor shall apply for the renewal and get the certification before the expiration of the product.

Nevertheless, GlobalPlatform reserves the right to withdraw a **Certificate** upon certain circumstances, such as a significant change in the applicable attack methods.

3.5.4 Publication

The decision about the confidentiality of the certification project rests with the Vendor.

Upon release of the **(Restricted) Certification Report** and **(Restricted) Certificate**, GlobalPlatform CB confirms with the Vendor whether the certification can be made public, in which case GlobalPlatform publishes them on GlobalPlatform's website.

3.5.5 Security Monitoring

GlobalPlatform CB through the SE Security Working Group security continuously monitors threats and security developments in the SE domain.

Where necessary and provided no non-disclosure agreement is compromised, GlobalPlatform CB may inform product vendors about newly discovered (residual) vulnerabilities of their certified products, thus enabling and supporting the product vendor to minimize subsequent risks, and to support their customers' risk management.

Under specific circumstances, GlobalPlatform CB may decide to withdraw or revoke, i.e. to shorten the validity period, a GlobalPlatform **(Restricted) Certificate**.

4 Laboratory Accreditation

4.1 General

To perform SE security evaluations under the GlobalPlatform SE Security Scheme, a laboratory must obtain and maintain GlobalPlatform accreditation, which implies complying with the requirements defined hereafter. To do so, the laboratory shall apply for accreditation by submitting the GlobalPlatform Laboratory Accreditation Request Form ([LAB R]) available from GlobalPlatform's website.

The accreditation process consists in the audit of the information provided by the laboratory to demonstrate compliance with the requirements. GlobalPlatform proceeds to accreditation renewal every two years or upon significant legal, organizational, or technical changes in the laboratory.

4.2 Accreditation Requirements

4.2.1 Purpose

This section identifies the set of general, business, and organizational requirements that a laboratory must meet in order to obtain and maintain GlobalPlatform accreditation for SE security evaluations.

4.2.2 General Requirements

4.2.2.1 GlobalPlatform Membership

[GR-01] The laboratory shall be either a GlobalPlatform Full Member or a GlobalPlatform Participating Member to the SE Committee, or it shall inherit such membership level from its parent organization.

4.2.2.2 Third-party Security Accreditations

[GR-02] The laboratory shall hold an ISO/IEC 17025 certificate issued by its national accreditation body that is valid at the date of audit.

> Note: The laboratory commits to inform GlobalPlatform of any change to the scope and validity date of the ISO/IEC 17025 certificate without delay.

[GR-03] The laboratory shall be listed in the SOG-IS website as "Qualified EAL1-7 for Smartcards and similar devices" by ITSEF.

> Note: The laboratory commits to inform GlobalPlatform of any change with regard to its qualification by a SOG-IS scheme.

4.2.3 Business Requirements

4.2.3.1 Financial

[BR-01] The laboratory shall conduct business in a manner that is consistent with the highest ethical standards and with practices that minimize risk.

[BR-02] The laboratory shall have a sound financial basis and be a part of a stable business organization.

[BR-03] The laboratory shall not have financial dependencies on any product vendor for which evaluation is being performed other than the product vendor's payment for the service provided.

[BR-04] The laboratory shall not have financial dependencies on any GlobalPlatform member with regards to performance of any GlobalPlatform SE evaluation activity unless permitted in writing by GlobalPlatform.

[BR-05] The laboratory shall be free of any past fraudulent or criminal activity.

4.2.3.2 Insurance

[BR-06] The laboratory shall maintain in effect, at its own expense, a general liability and professional liability insurance coverage that covers its responsibility up to $1M USD per occurrence or $2M USD aggregate. The laboratory is also meant to maintain all the insurances required by the applicable laws and regulations in the jurisdictions where the laboratory's services are performed.

4.2.3.3 Legal

[BR-07] The laboratory or the organization of which it is part shall be recognized as a legal entity and registered as a tax-paying business or as having a tax-exempt status or as a legal entity in some form with a national body.

[BR-08] The laboratory or the organization of which it is part shall be able to sign and abide by all applicable GlobalPlatform legal agreements, including GlobalPlatform **Security Laboratory Relationship Agreement**.

4.2.3.4 Public Communications

[BR-09] The laboratory shall agree to abide by GlobalPlatform's policy that testing performed at any GlobalPlatform Accredited Security Laboratory is acceptable for SE approval, and shall make no claims to the contrary in its communication and/or marketing material.

[BR-10] The laboratory shall not, under any circumstances, communicate or disclose to any third party, including to a Product Vendor, that a Product has or has not been certified by GlobalPlatform. GlobalPlatform, not the laboratory, shall be the final party to determine whether a particular Product satisfies the **SE Security Requirements**.

4.2.3.5 Independence

[BR-11] The laboratory shall be able to demonstrate its impartiality and its independence from the parties involved in the design or manufacturing of the Product(s) under evaluation.

[BR-12] The laboratory shall immediately notify GlobalPlatform CB in writing about any change to ownership or legal or management structure, in particular with regard to organizations involved in the design or manufacturing of Products, and the laboratory shall continuously fulfill all the obligations stipulated in the GlobalPlatform **Security Laboratory Relationship Agreement**.

[BR-13] The laboratory shall disclose to GlobalPlatform in writing when an individual Product Vendor represents more than 25% of the laboratory's total annual revenue for the laboratory's evaluation activities regardless of the scheme or evaluation methodology used.

[BR-14] The laboratory shall not evaluate a Product on which the laboratory or laboratory's staff has been involved in from design or manufacturing point of view, with the exception of functional or security quality assurance testing or debug sessions performed prior to the start of an official GlobalPlatform SE security evaluation.

[BR-15] The laboratory shall receive communication related to GlobalPlatform SE security evaluation only from GlobalPlatform CB.

4.2.3.6 Consistent Business Practices

[BR-16] The laboratory shall recognize the test results obtained by any other GlobalPlatform Accredited Security Laboratories during the evaluation of a GlobalPlatform certified Product, without any further investigation and without any discrimination regarding pricing for complementary testing.

4.2.4 Organizational Requirements

4.2.4.1 Quality Assurance

[OR-01] The laboratory shall have a quality system based upon ISO/IEC 17025 requirements, which includes documented procedures and processes to ensure a high quality of testing and test reproducibility.

[OR-02] The laboratory shall maintain an up-to-date library of reference material (guidance, procedures, books, papers, articles, etc.) on methods, standards, techniques, and equipment that are resident in the laboratory and that provide the information required for laboratory test performance.

[OR-03] The laboratory shall maintain up-to-date records of equipment maintenance.

4.3 Termination Process

4.3.1 Termination by the Laboratory

An Accredited Laboratory has the right to terminate the GlobalPlatform **Security Laboratory Relationship Agreement** at any time.

In order to terminate the **Security Laboratory Relationship Agreement** with GlobalPlatform, an Accredited Laboratory must notify GlobalPlatform CB in writing, present a termination plan with regard to current projects and ensure business continuity until the termination date.

Upon receipt of such a request, GlobalPlatform CB engages the termination procedures as defined in the Agreement and removes the laboratory’s name from the list of Accredited Laboratories on GlobalPlatform’s website.

Upon termination of its accreditation, the laboratory shall make available to GlobalPlatform CB all the test reports, test logs, and samples of the products evaluated within the GlobalPlatform scheme. The laboratory shall also promptly return to GlobalPlatform all GlobalPlatform property and all confidential information. Alternatively, if so directed by GlobalPlatform, the laboratory shall destroy all confidential information, and all copies thereof, in the laboratory’s possession or control, and shall provide a certificate signed by an officer of the laboratory that certifies such destruction in details acceptable to GlobalPlatform.

4.3.2 Suspension by GlobalPlatform

GlobalPlatform has the right to suspend at any time a laboratory’s accreditation due to the non-conformance with GlobalPlatform’s requirements.

Upon suspension, GlobalPlatform removes the name of the laboratory from the list of Accredited Laboratories on GlobalPlatform’s website and sets the requirements and the date by which an **Interim Proficiency Audit** must be completed.

4.3.3 Revocation by GlobalPlatform

GlobalPlatform has the right to revoke at any time a laboratory’s accreditation:

- Due to non-conformance with GlobalPlatform’s requirements
- If a laboratory has not performed testing of Products within the past two years
- If a laboratory fails to renew its accreditation before it expires

Revocation of accreditation automatically terminates the GlobalPlatform **Security Laboratory Relationship Agreement**. GlobalPlatform removes the laboratory’s name from the list of Accredited Laboratories on GlobalPlatform’s website.

Upon revocation of its accreditation, the laboratory shall make available to GlobalPlatform CB all the test reports, test logs, and samples of products evaluated within GlobalPlatform scheme. The laboratory shall also promptly return to GlobalPlatform all GlobalPlatform property and all confidential information. Alternatively, if so directed by GlobalPlatform, the laboratory shall destroy all confidential information, and all copies thereof, in the laboratory’s possession or control, and shall provide a certificate signed by an officer of the laboratory that certifies such destruction in details acceptable to GlobalPlatform.