GlobalPlatform Technology

Secure Element certification process

Version 1.0

Public release candidate

March 2019

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

This document describes the processes and requirements associated with the GlobalPlatform SE Certification Scheme. GlobalPlatform is the owner of the scheme, grants accreditation to evaluation laboratories and acts as the certification entity for all approvals relating to the security evaluation of SE and eUICC Products. The GlobalPlatform Security Evaluation Secretariat (SES) is the body 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 applicable documents including Operation Bulletins, the list of accredited laboratories and the certification fees' policy. In any case of difference in contents, the version of the document published in the website apply and supersedes 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.

1.1 Audience

This document is intended primarily for SE developers and manufacturers, collectively named SE Vendors, and 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.

1.2 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://www.globalplatform.org/specificationsipdisclaimers.asp. 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 following references are relevant to the SE Certification Process. Unless stated otherwise, the latest official release applies. Documents are accessible from either public or member GlobalPlatform website portal.

Table 1-1: Normative References

Standard / Specification	Description	Ref
	Joint Interpretation Library – Application of Attack Potential to Smartcards, version 2.9, January 2013	[JIL-AAPS]
	Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, version 2.2, January 2013	[JIL-AMSC]
893426.2	GlobalPlatform Security Laboratory Relationship Agreement Public	
893426.X	GlobalPlatform Laboratory Accreditation Request Form Public	
894365.2	GlobalPlatform Security Evaluation Agreement Public GlobalPlatform Exhibit B Product Evaluation Request Form Public	
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]
GPC_GUI_163	GlobalPlatform SE/eUICC Evaluation Methodology	[SE EM]
GPC_SPE_163	SE Protection Profile (core PP and PP-Modules) Public	[SE PP]
GPC_TEN_166	GlobalPlatform SE/eUICC Security Target Template Public	[SE ST]
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]
ISO/IEC 17025:2005	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]
SGP.16	M2M Compliance Process v1.0	[SGP.16]
SGP.24	RSP Compliance Process v2.0	[SGP.24]
SGP.25	Embedded UICC Protection Profile for Consumer Device v1.0 (BSI-CC-PP-0100-2018)	[SGP.25]

Table 1-2: Informative References

Standard / Specification	Description	Ref
GPC_SPE_095	GlobalPlatform Device Digital Letter of Approval	[DLOA]

1.4 Terminology and Definitions

The following meanings apply to SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY in this document (refer to [RFC 2119]):

- **SHALL** indicates an absolute requirement, as does **MUST**.
- **SHALL NOT** indicates an absolute prohibition, as does **MUST NOT**.
- **SHOULD** and **SHOULD NOT** indicate recommendations.
- **MAY** indicates an option.

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

Table 1-3: Terminology and Definitions

Term	Definition
GlobalPlatform Accredited Security Laboratory	A laboratory or test facility that has been accredited by GlobalPlatform to perform the security evaluation process described in the SE Certification Process document.
GlobalPlatform Security Laboratory Relationship Agreement	Agreement between GlobalPlatform and the accredited laboratory.
Product	A Secure Element or embedded UICC Product.
Product Evaluation Request Form	Form to be completed by the Product Vendor to request registration to the Secretariat and get the Registration Reference.
Registration Reference	Initial number issued to a Product Vendor by the Secretariat to start an evaluation process.
Product Vendor	An entity submitting a Product for assessment under the Evaluation Process, which acts as sponsor of the evaluation.
Risk Analysis Report	The report, prepared jointly by GlobalPlatform SES and the Product Vendor in the event the Product Vendor decides not to remedy the Product vulnerabilities identified as part of the Evaluation Process, and containing information for third-parties intending to use the Product.
Security Requirements	Collectively, the most recent version (unless GlobalPlatform SES specifies an earlier version) of the applicable Protection Profiles, SE/eUICC Evaluation Methodology, JIL Attack Catalog, and all amendments, modifications and upgrades as adopted by GlobalPlatform from time to time.
Restricted Security Certification Report	A *Security Certification Report* based on an *Evaluation Technical Report* that identifies residual vulnerabilities.
Security Certification Report	A document issued by GlobalPlatform SES which summarizes the results of a SE Product Evaluation and confirms the overall results, i.e. the Evaluation has been properly carried out, the GlobalPlatform Evaluation Methodology has been correctly applied and the conclusion of the *Evaluation Technical Report* are consistent with the adduced evidence.

Term	Definition
Restricted Security Evaluation Certificate	The written recognition and acknowledgement of restricted certification of a Product under the Evaluation Process, provided by GlobalPlatform SES to a Product Vendor for a Product that is found to have some residual vulnerabilities under the Evaluation Process.
Certificate Reference	A unique four-digit reference number that applies exclusively to the exact Product configuration described in the GlobalPlatform SES.
Certificate	A written statement that documents the decision of GlobalPlatform SES that a specified Product has demonstrated sufficient conformance to the Security Requirements as of its test date.

1.5 Abbreviations and Notations

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
DETR	Detailed Evaluation Technical Report
DLOA	Digital Letter of Approval
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
eUICC	Embedded UICC
IAR	Impact Analysis Report
PP	Protection Profile
PPs	All Protection Profiles supported by the SE scheme
PTP	Penetration Test Plan
SE	Secure Element
SES	Security Evaluation Secretariat
SESCN	Security Certificate Number
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation

1.6 Revision History

Table 1-5: Revision History

Date	Version	Description
July 2018	0.0.0.1	Draft
August 2018	0.0.0.4.	Board validated version
March 2019	0,0,0,5	Version for SE scheme launch board decision
March 2019	0.1	First published version

2 Principles of SE Certification Scheme

2.1 Processes and Actors

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

- Definition and maintenance of the **Security Requirements**, performed by GlobalPlatform SES and GlobalPlatform technical working groups;
- Laboratory accreditation, performed by the GlobalPlatform SES;
- Evaluation of Products, performed by GlobalPlatform Accredited Security Laboratories with the support of Product Vendors and monitored by GlobalPlatform SES;
- Issuance and management of Products' certificate, performed by GlobalPlatform SES.

The evaluation methodology [SE EM] is the result of a collaboration between GlobalPlatform and GSMA.

GlobalPlatform SES is also responsible to manage the synchronization with GSMA and the SOG-IS organization.

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

2.1.1 GlobalPlatform Security Evaluation Secretariat

GlobalPlatform is the owner of the GlobalPlatform SE Certification Scheme, grants accreditation to evaluation laboratories and acts as the certification entity for all approvals relating to the security of the Products.

GlobalPlatform SES is the body that operates the scheme and is responsible for enforcing the GlobalPlatform SE Certification Process. A GlobalPlatform Director is appointed as GlobalPlatform's representative in the Security Evaluation Secretariat.

GlobalPlatform Security Evaluation Secretariat is in charge of:

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

More precisely, the role of GlobalPlatform SES in the evaluation and certification processes (cf. chapter 3) consists of the following activities:

- Provide the Security Evaluation Agreement to the Vendor;
- Validate the Product Evaluation Request Form and companion documentation and provide a registration reference;
- Validate the Penetration Test Plan and companion documentation;
- Validate the (Detailed) Evaluation Technical Reports (DETR and ETR);
- Establish the Risk Analysis Report with the Product Vendor (if applicable);
- Write a (Restricted) Security Evaluation Certificate;
- Issue (Restricted) Security Certification Report upon successful evaluation of the Product;
- Publish certificates in the Certification Scheme web page unless otherwise decided by the Product Vendor.

Vendors shall contact GlobalPlatform SES at secertification@globalplatform.org or any other contact address provided in GlobalPlatform's website.

2.1.2 GlobalPlatform Accredited Security Laboratories

GlobalPlatform Accredited Security Laboratories for the evaluation of SE Products must comply with the criteria set out in section 4.1 of this document, which requires being a member of GlobalPlatform and "Qualified EAL1-EAL7 for Smartcards and similar devices" by the SOG-IS organization.

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.

GlobalPlatform Accredited Security Laboratories are responsible for:

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

Accredited Laboratories are active contributors of the scheme through their participation to the GlobalPlatform's technical working groups.

2.1.3 Product Vendors

Product Vendors request the security evaluation of their Products to GlobalPlatform SES 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 select the evaluation type (Full, Delta, Fast-track or Reassessment);
- Providing the Security Target of their Product;
- 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;
- Informing 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 the scope of GlobalPlatform SE Certification Scheme.

2.1.4 SE Scheme Users

SE Scheme User stands for any actor that relies on security features as stated in the PPs, for instance a digital service provider or a device integrator (OEM)..

When relying on a certified Product, the SE scheme User is responsible for checking the Security Evaluation Certificate and corresponding Security 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 which are covered by the certificate;
- The assumptions about the operational environment where the Product will be used or integrated;
- The limitations in case of a **Restricted Security Evaluation Certificate.**

2.2 Security Requirements

The SE scheme is built on a set of specifications called **Security Requirements**, which is the basis of the SE Certification Scheme and contains

- This document;
- The Joint SE Evaluation Methodology [SE EM], which relies on JIL attack methods documentation [JIL-AAPS] and [JIL-AMSC];
- The SE Protection Profile [SE PP], the Embedded UICC Protection Profile [SGP.05] , the Embedded UICC for Consumer Device Protection Profile [SGP.25], or a certified Protection Profile applicable to GlobalPlatform Card Technology-based products with an HW at EAL4+ or higher commonly named PPs;

These documents are synchronized by the GlobalPlatform SES and maintained by the technical security working groups of GlobalPlatform and GSMA composed of SE and security experts, 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.

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

2.2.1 Certification Process Document

Owner: GlobalPlatform Security Evaluation Secretariat.

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

Audience: Laboratories, Product Vendors, SE scheme Users.

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

2.2.2 Protection Profiles

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

Content: Each PP defines the Target of Evaluation (TOE) and its assets, the threat model, the assumptions, the Security Functional Requirements (SFRs) and the applicable evaluation assurance level.

Updates of a Protection Profile may be triggered by:

- Additional features;
- Update of the specifications with security impact;
- New attack methods, especially those included in evolutions [JIL-AMSC][JIL-AMSC]and [JIL-AAPS].

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

Protection Profile Approval/Certification:

- Common Criteria evaluation and certification of the PPs' initial version ;
- Common Criteria evaluation and certification of major updates of the PPs.

Audience: Laboratories, Product Vendors, SE scheme Users.

Distribution: The applicable Protection Profiles are available in the public website www.globalplatform.org.or and in Common Criteria portal https://www.commoncriteriaportal.org.

2.2.3 Evaluation Methodology

Owner: GlobalPlatform SE Security Working Group and GSMA.

Content: The document [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.

Updates of the Evaluation Methodology may be triggered by:

- Feedback from the field;
- Modification of the scope, acceptable form factors, etc.
- Reuse of results from other evaluation schemes;
- GlobalPlatform or GSMA specification update;
- Attack methods update;
- Protection Profiles update.

Audience: Laboratories and Product Vendors.

Distribution: The Evaluation Methodology is available to GlobalPlatform Members through the member website https://members.globalplatform.org and to interested Product Vendors upon request to the Security Evaluation Secretariat.

2.2.4 Attack Methods

Owner: JIL Working Group

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

Updates of the Attack Catalog may be triggered by:

- New attacks the field or new attack technics;
- Protection Profiles 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 [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.

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

2.4 Security Evaluation

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

The Evaluation Methodology seeks to optimize the cost and time of evaluation work. 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.

2.4.1 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 PPs 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 will issue a recommendation with regard to the type of evaluation that should be performed. The Vendor will then submit the IAR and the recommendation statement to GlobalPlatform SES, which shall decide 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 the GlobalPlatform SES, which shall decide on the application of Fast-track evaluation process. The principle is that any security change in the product shall give 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 **Security Requirements**.

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

2.4.2 Reuse of Evaluation Work

GlobalPlatform SES allows reusing evaluation results through Delta, Fast-track and Reassessment evaluation processes. Moreover, GlobalPlatform allows reusing evaluation results from other schemes upon request. Such decision is performed in a case-by-case basis.

The inputs must be unambiguously identified in the **Product Evaluation Request Form**.

2.5 Security Certification

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

In case potential vulnerabilities are found during the evaluation, GlobalPlatform may either deny to certify the Product or issue a **Restricted Security Evaluation 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) Security Evaluation 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** (SESCN) 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.

2.5.1 Recognition of Common Criteria Certificates

GlobalPlatform has defined the conditions under which Common Criteria (CC) certificates of products issued by a CC certification body could be reused:

1. The CC certification scheme is participating to the SOG-IS organization
2. The Security Target of the CC certified product claims conformance with valid versions of the applicable Protection Profiles at the date of certification;
3. The Security Target claims conformance with the assurance components of the Evaluation Assurance Level defined in the PPs;
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 SES is informed of the issuance of the CC Certificate within ten (10) days from the issuance of the Certificate;
7. GlobalPlatform SES receives the Security Target and the CC Certification Report within ten (10) days from the issuance of the Certificate;
8. The CC scheme supports GlobalPlatform SES 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.

2.5.2 Risk Management

SE scheme 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 the 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.

SE scheme 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 will likely succeed in compromising the Product's assets. A secure system must implement defenses at all levels, and SE scheme 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 to the User's risk analysis.

In the event that a Product only receives a GlobalPlatform **Restricted Security Evaluation 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 SE scheme Users. SE scheme 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 Certification 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 Product Evaluation Request

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

GlobalPlatform SES shall provide its public key to protect the product-related documentation that is required from the vendor and from the lab during the entire certification project.

GlobalPlatform SES will then examine the evaluation request and related documents and will notify the vendor about the decision: acceptance, denial or request of complementary information or update of the documents.

Upon acceptance, GlobalPlatform and the Product Vendor shall sign the GlobalPlatform Security Evaluation Agreement. GlobalPlatform SES will then register the certification request and provide a unique registration number for use in all communications up to the certification decision.

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 in GlobalPlatform's website or not. The publication choice may be modified at the end of the certification process.

3.1.2 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 GlobalPlatform SE scheme.

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;
- The laboratory has received from the Vendor all the inputs that are necessary to perform the evaluation as defined in [SE EM].

3.1.3 Product Assessment

The laboratory shall perform the Product evaluation as defined in [SE EM], which consists of a vulnerability analysis phase (documentation review, source code inspection and security functional testing) and a testing phase of security functionality that addresses the attack methods described JIL documents [JIL-AMSC] and [JIL-AAPS].

The GlobalPlatform SES shall review the Penetration Test Plan (PTP) and shall confirm 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 3 months, provided the Product complies with GlobalPlatform's and/or GSMA specifications and all the necessary evaluation inputs are available at the starting date (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 3 months. More time might be necessary where, for instance, the product requires security updates or either the laboratory or GlobalPlatform SES 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, at its own discretion and under special circumstances, may extend such period.

3.1.4 Evaluation Reports

After evaluation, the GlobalPlatform Accredited Security Laboratory shall issue a **DETR** and an **ETR** as defined in [SE EM]. DETR and ETR 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 PPs, 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 PPs, which are 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 PPs or with an attack potential that goes beyond the requirements and does not comply with the threshold defined in the PPs.

The ETR is transmitted to the Vendor and to GlobalPlatform SES. The DETR is transmitted to the Vendor and is available to GlobalPlatform SES upon request during the certification project or later at the time of an audit of the laboratory.

3.1.5 Evaluation Reports Review

The GlobalPlatform SES shall review the ETR and shall make a certification decision, which may range from the acceptance of the results without further activities to the request of the DETR or additional information or testing.

If the GlobalPlatform SES considers that the evaluation provides sufficient assurance that the Product complies with the GlobalPlatform Security Requirements, the GlobalPlatform SES writes a GlobalPlatform Security Certification Report, which is transmitted to the laboratory and to the vendor for review prior official release.

3.1.6 Risk Analysis Report

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

1. GlobalPlatform SES proposes to issue a SE **Restricted Security Evaluation Certificate**, which requires the agreement of the Vendor to prepare a joint Risk Analysis Report containing information for Users of the Product;

2. GlobalPlatform SES denies 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 SES reserves its final authority over its content to ensure that SE scheme Users will receive reliable information derived from the SE evaluation, which is meaningful to the risk assessment of their SE services or deployments. GlobalPlatform SES will then write a GlobalPlatform Restricted Security Certification Report, including a reference to the Risk Analysis Report, and transmit it to the laboratory and to the vendor for review prior official release.

3.1.7 Security Evaluation Certificate Issuance

GlobalPlatform SES will issue the (Restricted) Security Evaluation Certificate without delay upon edition of the (Restricted) Security Certification Report. The certificate shall contain the Security Certificate Number (SESCN), a unique four-digit reference number identifying the Product that has been evaluated and certified.

The management of the life-cycle of (Restricted) Security Evaluation Certificate and the publication rules are described in section 3.5.

3.1.8 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:
  - The same name and version used in the request form can be used in the Security Target;
  - The identification of 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 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 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's components, as evaluated by the laboratory;
- The DETR and ETR must provide the real Product name and version, as per the final Security Target;
- The DETR and ETR must identify all the versions of TOE's components that have been audited/tested during the evaluation;
- The DETR and ETR must identify the final versions of the TOE components upon which the evaluation verdict has been made, as per the final Security Target.

At certification time:

- The (Restricted) Security Certification Report and corresponding (Restricted) Certificate shall include the real Product and TOE components identification, as per final Security Target, ETR and DETR;
- The (Restricted) Security 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 shall prepare an **Impact Analysis Report** (IAR) describing all the hardware and software changes to the original certified Product and their security impact and shall submit the IAR to the selected laboratory for review. The laboratory shall assess the feasibility of the Delta evaluation and shall issue a recommendation. Both the IAR and the laboratory's recommendation shall be provided to GlobalPlatform SES together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform SES will then examine the Delta evaluation request and will notify the Vendor about the decision: acceptance, denial or request of complementary information.

The Delta evaluation steps are the same as in a Full evaluation. Upon successful evaluation, GlobalPlatform SES shall issue a Derived Certificate for the new Product, which shall reference the original Certificate.

3.3 Fast-track Evaluation

In order to apply for a Fast-track evaluation of a new Product, the Vendor shall prepare 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 shall be provided to GlobalPlatform SES together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform SES will then examine the Fast-track evaluation request and will notify the Vendor about the decision: acceptance, denial or request of complementary information.

Upon acceptance of Fast-track evaluation, GlobalPlatform SES shall perform 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 shall prepare 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 shall be provided to GlobalPlatform SES together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform SES will then examine the Reassessment evaluation request and will notify the Vendor about the decision: acceptance, denial or request of complementary information.

Upon acceptance of Reassessment evaluation, GlobalPlatform SES shall perform all the technical and administrative steps (same as in a Delta evaluation) to issue the renewal Certificate of the Product, with an extended expiry date.

3.5 Certificate Management

3.5.1 Certificate

A GlobalPlatform Security Evaluation Certificate confirms that the Product identified in the certificate has undergone security evaluation by an Accredited Laboratory against the Protection Profile requirements as defined in the Evaluation Methodology, and that no significant residual vulnerability has been discovered. It includes:

- Certificate identification number;
- Identification of the TOE;
- Identification of the Vendor;
- PPs compliance claim;
- Identification of the Accredited Laboratory that performed the evaluation;
- Reference of the **Security Certification Report.**

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

A **GlobalPlatform Security Certification Report** includes:

- Certification Report identification number;
- Certification Report issuance date;
- 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 or a Fast-track evaluation, the reference to the original Certificate and Certification Report shall be included.

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

3.5.2 Restricted Certificate

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

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

A GlobalPlatform Restricted Security 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) Security Evaluation Certificate** issued from a Full evaluation is valid for five (5) years from the certification date.

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

A successful Reassessment Evaluation shall give 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) Security Certification Report, GlobalPlatform SES shall confirm with the Vendor whether the certification can be made public, in which case GlobalPlatform will publish the (Restricted) Security Evaluation Certificate and the corresponding Certification Report in GlobalPlatform's website.

3.5.5 Security Monitoring

The GlobalPlatform SES through the SE Working Group security shall continuously monitor threats and security developments in SE domain

Editor's Note : Contribution to JIL be added here if an agreement is found

Where necessary and provided no non-disclosure agreement is compromised, GlobalPlatform SES 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 SES may decide to withdraw or revoke, i.e. to shorten the validity period, a GlobalPlatform **(Restricted) Security Evaluation Certificate**.

4 Laboratory Accreditation

To perform Security evaluations under the GlobalPlatform SE 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 corresponding request form 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 will proceed to accreditation renewal every two years or upon significant legal, organizational or technical changes in the laboratory.

4.1 Accreditation Requirements

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

4.1.1 General Requirements

4.1.1.1 GlobalPlatform Membership

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

4.1.1.2 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 any change on the scope and validity date of the ISO/IEC 17025 certificate without delay.

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

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

4.1.2 Business Requirements

4.1.2.1 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.

4.1.2.2 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 laboratory's services are performed.

4.1.2.3 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**.

4.1.2.4 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 **Security Requirements**.

4.1.2.5 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 the GlobalPlatform SES 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 Security Evaluation.

[BR-15] The laboratory shall receive communication related to GlobalPlatform Security Evaluation only from GlobalPlatform SES.

4.1.2.6 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.

4.1.3 Organizational Requirements

4.1.3.1 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.

4.2 Termination Process

4.2.1 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 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 will engage the termination procedures as defined in the Agreement and remove the laboratory’s name from the list of Accredited Laboratories in GlobalPlatform’s website.

Upon termination of its accreditation, the laboratory shall make available to GlobalPlatform all the test reports, test logs and samples of the 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.

4.2.2 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, GlobalPaltform will remove the name of the laboratory from the list of Accredited Laboratories in GlobalPlatform’s website and will set the requirements and the date by which an **Interim Proficiency Audit** must be completed.

4.2.3 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 will remove the laboratory’s name from the list of Accredited Laboratories in GlobalPlatform’s website.

Upon revocation of its accreditation, the laboratory shall make available to GlobalPlatform 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.