GlobalPlatform

TEE Certification Process

Version 1.1

Public Release

September 2017

Document Reference: GP_PRO_023

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

Figures

Tables

1 Introduction

This document describes the processes and requirements associated with the GlobalPlatform TEE 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 TEE Products. The GlobalPlatform Security Evaluation Secretariat is the body that operates the scheme and is responsible for enforcing the GlobalPlatform **TEE Certification Process**, as defined in this document.

The GlobalPlatform website (today at http://www.globalplatform.org/TEECertification.asp) provides the latest applicable documents including Operation Bulletins, the list of accredited laboratories and the certification fee policy. In case of differences, the versions of the documents published in 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 TEE Product evaluation and certification processes.
- Chapter 4 presents the laboratory accreditation requirements and related processes.
- Annex A presents the extension of the TEE Certification Scheme to TEE Parts.

1.1 Audience

This document is intended primarily for TEE Vendors, TEE Users and laboratories that intend to perform TEE security evaluations.

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 TEE Certification Process. Unless stated otherwise, the last official release applies. Documents are accessible from either public or member GlobalPlatform website portal.

Table 1-1: Normative References

Standard / Specification	Description	Ref
GPD_SPE_009	GlobalPlatform TEE System Architecture Public	[TEE SA]
GPD_SPE_010	GlobalPlatform TEE Internal API Specification Public	[TEE IAPI]
GPD_SPE_007	GlobalPlatform TEE Client API Specification Public	[TEE CAPI]
GPD_SPE_021	GlobalPlatform Device Committee TEE Protection Profile (PP-base and PP-modules) Public	[TEE PP]
GPD_NOT_051	Application of Attack Potential to Trusted Execution Environment – Confidential version (Attack Catalog)	[TEE AP]
GPD_GUI_044	GlobalPlatform TEE Evaluation Methodology Member document Available under request to non-member TEE Vendors	[TEE EM]
GPD_TEN_045	GlobalPlatform TEE Security Target Template Public	[TEE ST]
GPD_SPE_050	GlobalPlatform TEE Common Automated Tests Member document Available under request to non-member TEE Vendors as amended by: GlobalPlatform TEE Security Test Suite Member document	[TEE CAT]
GP_GUI_028	GlobalPlatform Accreditation Guidelines and Audit Plan Member document	[TEE LAG]
894365.2	GlobalPlatform Security Evaluation Agreement Public	
	GlobalPlatform Exhibit B Product Evaluation Request Form Public	
893426.2	GlobalPlatform Security Laboratory Relationship Agreement Public	
	GlobalPlatform Laboratory Accreditation Request Form Public	
ISO/IEC 17025:2005	General requirements for the competence of testing and calibration laboratories	[ISO 17025]

Table 1-2: Informative References

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

1.4 Terminology and Definitions

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 TEE Certification Process document.
GlobalPlatform Qualified Auditor	An independent expert qualified by GlobalPlatform to perform accreditation audits of security evaluation laboratories.
GlobalPlatform Security Laboratory Relationship Agreement	Agreement between GlobalPlatform and the accredited laboratory.
Product	A TEE Product, that is, a device or System-on-Chip (SoC) embedding a TEE, submitted for assessment under the Evaluation Process.
Product Evaluation Request Form	A completed written request for security evaluation of a Product by a Product Vendor, through the Evaluation Process.
Product Registration Number	A unique number identifying the TEE Product, assigned at the start of the 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 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 specifies an earlier version) of the TEE Protection Profile, TEE Evaluation Methodology and TEE Attack Catalog, and all amendments, modifications and upgrades as adopted by GlobalPlatform from time to time.
TEE Restricted Security Certification Report	A *TEE Security Certification Report* based on a *Technical Evaluation Report* that identifies residual vulnerabilities.
TEE Restricted Security Evaluation Certificate	The written recognition and acknowledgement of restricted certification of a Product under the Evaluation Process, provided by GlobalPlatform to a Product Vendor for a Product that is found to have some residual vulnerabilities under the Evaluation Process.
TEE Security Certificate Number	A unique four-digit reference number that applies exclusively to the exact TEE Product configuration described in the GlobalPlatform TEE Security Evaluation Certificate.

Term	Definition
TEE Security Certification Report	A document issued by GlobalPlatform which summarizes the results of a TEE 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 *Technical Evaluation Report* are consistent with evidence adduced.
TEE Security Evaluation Certificate	A written statement that documents the decision of GlobalPlatform that a specified Product has demonstrated sufficient conformance to the GlobalPlatform security requirement as of its test date.

1.5 Abbreviations and Notations

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
DLOA	Digital Letter of Approval
DTER	Detailed TEE Evaluation Report
EAL	Evaluation Assurance Level
IAR	Impact Analysis Report
OS	Operating System
PP	Protection Profile
REE	Rich Execution Environment
SES	Security Evaluation Secretariat
SFR	Security Functional Requirement
SoC	System-on-Chip
ST	Security Target
TA	Trusted Application
TEE	Trusted Execution Environment
TEESCN	TEE Security Certificate Number
TER	TEE Evaluation Report
TOE	Target Of Evaluation

1.6 Revision History

Table 1-5: Revision History

Date	Version	Description
July 2015	1.0	Initial Public Release
September 2017	1.1	Public Release Editorial changes and harmonization of contents with regards to current processes (all sections). New structure of the document that gathers evaluation and certification topics in two consecutive chapters (2 and 3) instead of (2, 3, and 5): o Previous Chapter 3 becomes section 2.2. o Previous Chapter 5 becomes Chapter 3. Clarification of residual vulnerabilities (sections 3.1.4 and 3.1.6). Labelling of laboratory accreditation requirements (section 4.3). New sections: o 2.2.4 Security Functional Test Suite o 3.1.8 Product Identification o 4.1.4 Incremental Audit o Annex A for the certification of TEE Parts Delta and Fast-Track evaluation sections completed.

2 Principles of TEE Certification Scheme

2.1 Processes and Actors

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

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

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

2.1.1 GlobalPlatform Security Evaluation Secretariat

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

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

GlobalPlatform Security Evaluation Secretariat (SES) is in charge of:

- Definition and maintenance of the **TEE Certification Process** (this document);
- Definition and maintenance of **TEE Security Requirements** (see section 2.2);
- Laboratory accreditation and management (see Chapter 4);
- TEE Vendor evaluation request validation and evaluation monitoring (see Chapter 3);
- Certificate issuance, publication, and management (see section 3.4).

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

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

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

2.1.2 GlobalPlatform Qualified Auditors

GlobalPlatform Qualified Auditors are independent experts qualified by GlobalPlatform to perform accreditation audits of security evaluation laboratories.

More precisely, the role of GlobalPlatform Qualified Auditors consists of the following activities (see section 4.2):

- Define the Accreditation Audit plan;
- Perform the audit of the documentation provided by the laboratory to demonstrate the compliance with the Laboratory Accreditation Requirements defined in section 4.3;
- Perform the visit of the laboratory's premises;
- Write the **Preliminary Audit Report** and analyze the laboratory's **Corrective Actions Plan** (if applicable);
- Write the **Final Audit Report** and provide to GlobalPlatform SES the recommendation about the accreditation of the laboratory.

2.1.3 GlobalPlatform Accredited Security Laboratories

GlobalPlatform Accredited Security Laboratories are allowed to perform TEE Security Evaluations.

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 to 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 SES in case of change of accreditation conditions, e.g. changes to the expert staff, ownership or management structure, legal status, locations, third-party accreditations;
- Evaluating TEE Products against the **TEE Security Requirements** using the TEE Evaluation Methodology [TEE EM];
- Writing **Detailed TEE Evaluation Report (DTER)** and extracting the **TEE Evaluation Report (TER).**

2.1.4 TEE Vendors

TEE Vendors request the security evaluation of their Products to GlobalPlatform Security Evaluation Secretariat, provides all the necessary materials to the laboratory. TEE 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 or Fast-track);
- Providing the **Security Target** of their Product, compliant with the GlobalPlatform TEE Protection Profile [TEE PP];
- Providing the **Impact Analysis Report** of their Product, if applicable;
- Providing the information and material listed in the TEE Evaluation Methodology [TEE EM] to the GlobalPlatform Accredited Security Laboratory;

- Communicating about any previous evaluation or certification of the TEE Product.

The relationship between GlobalPlatform and TEE 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 TEE Certification Scheme.

2.1.5 TEE Users

TEE User stands for any actor that relies on TEE security features as stated in the TEE Protection Profile [TEE PP], for instance a digital service provider or a device integrator (OEM).

When relying on a certified TEE Product, the TEE User is responsible for checking the **TEE Security Evaluation Certificate** and **TEE Security Certification Report**:

- Type of the certificate (unrestricted or restricted);
- Scope of the certification, i.e. the security features of the TEE Product that have been evaluated and which are covered by the certificate;
- Assumptions about the operational environment where the TEE Product will be used or integrated;
- Limitations in case of a **TEE Restricted Security Evaluation Certificate**.

2.2 TEE Security Requirements

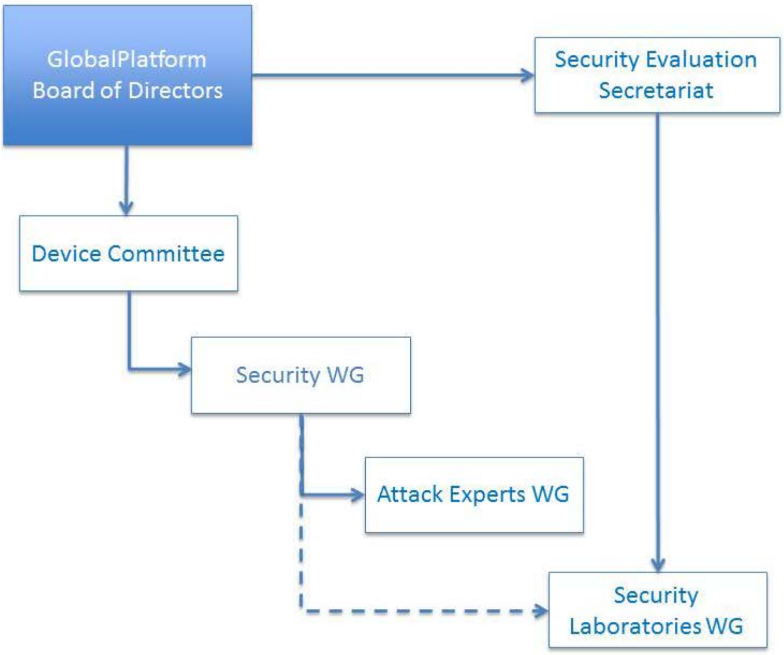
GlobalPlatform defines the set of specifications, called **TEE Security Requirements**, which is the basis of the TEE Certification Scheme and contains this document, the TEE Protection Profile and related PP-Modules [TEE PP], the TEE Evaluation Methodology [TEE EM], the Security Functional Test Plan (as described in TEE Common Automated Tests [TEE CAT]), and some supporting documents referenced therein**.**

These documents are managed by the GlobalPlatform Security Evaluation Secretariat and three technical working groups composed of TEE 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 TEE Certification Process.

Figure 2-1 presents the relationships between GlobalPlatform working groups involved in the definition of the **TEE Security Requirements**.

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

Figure 2-1: GlobalPlatform Organization for TEE Certification



2.2.1 Certification Process Document

Owner: GlobalPlatform Security Evaluation Secretariat.

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

Audience: Laboratories, TEE Vendors, TEE Users.

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

2.2.2 Protection Profile

Owner: GlobalPlatform TEE Security Working Group.

Content: The TEE Protection Profile [TEE PP] consists of a base-PP and a collection of optional PP-Modules defined as per of the Common Criteria rules. The [TEE 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, i.e. EAL2+ with TEE-specific vulnerability analysis AVA_TEE.2. It contains an extract of the Attack Catalog [TEE AP].

Updates of the Protection Profile may be triggered by:

- Additional features in the TEE specifications;
- Specification update that has an impact on security;
- New attacks from the TEE Attack Experts Working Group.

The update can give rise to new PP-modules or to modification of the existing base-PP or PP-modules.

Protection Profile Approval/Certification:

- The initial version of the TEE Protection Profile has been evaluated and certified in the Common Criteria scheme;
- Major updates will also be evaluated in the Common Criteria scheme.

Audience: Laboratories, TEE Vendors, TEE Users.

Distribution: The applicable Protection Profile(s) is available in the public website www.globalplatform.org.

2.2.3 Evaluation Methodology

Owner: GlobalPlatform Security Laboratories Working Group.

Content: The document [TEE EM] describes the process and requirements for vendors and GlobalPlatform Accredited Security Laboratories to perform TEE evaluations conformant with the Security Functional Requirements and assurance level defined in the TEE Protection Profile [TEE PP].

Updates of the Evaluation Methodology 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;
- TEE specification update;
- Attack Catalog [TEE AP] update;
- TEE Protection Profile [TEE PP] update.

Audience: Laboratories and TEE Vendors.

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

2.2.4 Security Functional Test Suite

Owner: GlobalPlatform TEE Security Laboratory Working Group.

Content: The document [TEE CAT] defines the set of security functional test cases that must be run on TEE Products during the vulnerability analysis phase of the evaluation. Updates of the TEE security test suite may be triggered by:

- Updates to the TEE specifications;
- TEE Protection Profile [TEE PP] evolution.

Audience: Laboratories and TEE vendors.

Distribution: The TEE security test suite is freely available for GlobalPlatform members from the website. It is also available under commercial conditions to non-members.

2.2.5 Attack Catalog

Owner: GlobalPlatform TEE Attack Experts Working Group.

Content: The document [TEE AP] illustrates the set of attacks that must be considered in a TEE evaluation.

Updates of the Attack Catalog may be triggered by:

- New attacks the field or new attack technics;
- TEE Protection Profile [TEE PP] scope evolution.

Audience: Laboratories and TEE vendors.

Distribution: The distribution of the Attack Catalog is restricted to GlobalPlatform TEE Attack Experts Working Group members. GlobalPlatform manages the communication between the TEE Attack Experts Working Group and external entities.

2.3 Target of Evaluation

The TOE is the Trusted Execution Environment as defined by GlobalPlatform[1] (see the GlobalPlatform TEE System Architecture [TEE SA] and the TEE API specifications, including [TEE CAPI] and [TEE IAPI]); that is, an execution environment that provides secure initialization, isolation from the Rich Execution Environment (REE), isolation between Trusted Applications (TAs), Trusted Storage, Random Number Generation (RNG), cryptographic operations, etc.

The TOE comprises the hardware, firmware and software components and mechanisms that provide such security features: The System-on-Chip (SoC), the boot firmware, the Trusted OS and drivers, the communication agent with the REE and the APIs exported to the TAs running on top of the Trusted OS.

The TOE does not comprise the TAs, the REE and its applications.

The guidance for the secure configuration and usage of the TOE is an integral part of the evaluation.

In GlobalPlatform TEE Certification Scheme, the TOE's form-factor is either a final device or an SoC. At GlobalPlatform's discretion, a product family can be evaluated once. The variations within a family that may be evaluated at once rests with GlobalPlatform.

The TOE is the part of TEE Product that is in the scope of the vulnerability analysis and testing as defined in the Evaluation Methodology.

[1] Functional compliance with GlobalPlatform TEE API specifications is not mandatory. Nevertheless, compliance has a positive impact on the evaluation and certification workplans.

2.4 Security Evaluation

The GlobalPlatform TEE Certification Process requires an independent evaluation of the TEE Product against the [TEE PP] requirements and the support of the TEE 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 and fast-track evaluations, families of TEE Products can be evaluated and certified in an incremental approach where the design is evaluated once and the paperwork overhead is reduced. The document [TEE EM] defines the inputs required from the TEE Vendor and the analysis and testing steps that the laboratory must perform to assess the security mechanisms of the TEE Product. The Evaluation Methodology achieves a balance between automated black-box testing and white-box testing. The laboratory carries out an independent vulnerability analysis that allows to derive a specific set of relevant penetration tests based on the TEE Product characteristics.

2.4.1 Types of Evaluations

GlobalPlatform security certification scheme relies on three types of evaluations:

- Full evaluation: It applies to TEE 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 [TEE PP] and the selected PP-modules. The Evaluation Methodology has been designed to enable GlobalPlatform Accredited Security Laboratories to perform evaluation of TEE Products in three (3) months provided the TEE complies with GlobalPlatform APIs and the Vendor grants access to the TEE source code and to a sufficient number of boards and/or devices.
- 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 Security Evaluation Secretariat, which shall make a decision 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 Security Evaluation Secretariat, which shall make a decision on the application of Fast-track evaluation process. The principle is that any security change shall give rise to a Full or a Delta evaluation.

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

2.4.2 Reuse of Evaluation Work

GlobalPlatform allows reusing evaluation results through Delta and Fast-track evaluation processes. Moreover, GlobalPlatform allows reusing evaluation results from other schemes upon request. The decision is performed in a case-by-case basis. For example, such reuse may concern:

- Common Criteria security evaluation compliant with [TEE PP];
- Audits of development and manufacturing sites performed by recognized organizations against international standards, e.g. ISO 27001 and PCI DSS.

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 TEE Certification Scheme is a GlobalPlatform **TEE Security Evaluation Certificate**.

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

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

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

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

Certified TEE 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:

- The CC certification scheme has signed an MOU with GlobalPlatform, which includes the participation to the TEE Attack Experts Working Group;
- The Security Target of the CC certified product claims conformance with a valid version of GlobalPlatform TEE Protection Profile at the date of certification;
- The Security Target claims conformance with the assurance components of the Evaluation Assurance Level EAL2+ defined in GlobalPlatform TEE Protection Profile;
- The evaluation of the TEE product against the TEE-specific EAL defined in the [TEE PP] requirements has been made using a valid version of GlobalPlatform Application of Attack Potential to Trusted Execution Environments;
- The Common Criteria TEE evaluation has been performed by a GlobalPlatform Accredited Laboratory;
- GlobalPlatform Security Evaluation Secretariat (SES) is informed of the issuance of the Common Criteria TEE Certificate within ten (10) days from the issuance of the Certificate;
- GlobalPlatform SES receives the Security Target and CC Certification Report within ten (10) days from the issuance of the Certificate;
- The CC scheme supports GlobalPlatform SES risk management activities related to potential vulnerabilities of the CC-certified TEE Product, in the event of new attacks in the field or new attack methods.

2.5.2 Risk Management

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

TEE 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 TEE 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 TEE Certification Process aims at providing an independent statement about the resistance level and the potential vulnerabilities of the TEE Product, which can be integrated to the User's risk analysis.

In the event that a TEE Product only receives a GlobalPlatform **Restricted Security Evaluation Certificate**, the TEE Vendor should be in a position to explain the reasons, and to offer guidance about the potential risks to the implementation plans of TEE Users. TEE 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 TEE 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 Security Evaluation Secretariat the **Product Evaluation Request Form**, containing the product identification details and the laboratory name, together with the TEE Product Security Target[2] and the list of evidences of previous independent security evaluations/certifications carried out on the product.

GlobalPlatform Security Evaluation Secretariat 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 Security Evaluation Secretariat 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 will then register the certification request and provide a unique registration number for use in all communications up to the certification decision.

The TEE 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 TEE Product. The contractual phase and the terms of the contract are out of scope of GlobalPlatform scheme.

In order to start the evaluation, the laboratory must provide the evaluation workplan provide to GlobalPlatform Security Evaluation Secretariat. 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 Security Evaluation Secretariat 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 the TEE Evaluation Methodology [TEE EM].

GlobalPlatform Security Evaluation Secretariat shall organize a kick-off meeting with the laboratory and the vendor and shall monitor the evaluation progress.

[2] The ST shall comply with the template provided by GlobalPlatform [TEE ST], which is based on the [TEE PP].

3.1.3 Product Assessment

The laboratory shall perform the TEE Product evaluation as defined in the TEE Evaluation Methodology [TEE EM], which consists of a vulnerability analysis phase (documentation review, source code inspection and automated security functional testing) and a testing phase of security functionality that addresses the attack methods described in the Attack Catalog [TEE AP].

The typical duration of a GlobalPlatform evaluation is three (3) months, provided the TEE Product complies with GlobalPlatform's specifications and all the necessary evaluation inputs are available at the starting date (e.g. security target, source code, test boards). Such a duration applies for one product version.

Nevertheless, there is no formal obligation in general to perform the evaluation in three (3) months. More time might be necessary where, for instance, the product requires security updates or either the laboratory or GlobalPlatform 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 one (1) year 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 **Detailed TEE Evaluation Report (DTER)** and a **TEE Evaluation Report (TER)** as defined in [TEE EM]. DTER and TER shall contain the description and outcomes of the vulnerability analysis and testing as well as:

- The laboratory's verdict with regard to the TEE Product's resistance to attackers with attack potential as defined in the [TEE PP], provided the use of the TEE 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 [TEE PP] that are covered by dedicated recommendations given in the TEE 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 [TEE PP] or with an attack potential that goes beyond the requirements and does not comply with the threshold defined in the [TEE PP].

The TER is transmitted to the Vendor and to GlobalPlatform Security Evaluation Secretariat. The DTER is transmitted to the Vendor and is available to GlobalPlatform Security Evaluation Secretariat 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 Security Evaluation Secretariat shall review the **TER** and shall make a certification decision, which may range from the acceptance of the results without further activities to the request of the **DTER** or additional information or testing.

If the GlobalPlatform Security Evaluation Secretariat considers that the evaluation provides sufficient assurance that the Product complies with the **GlobalPlatform TEE Security Requirements**, the **GlobalPlatform Security Evaluation Secretariat** writes a **GlobalPlatform TEE 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 Security Evaluation Secretariat 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 or by the Vendor. Following such analysis, two situations may arise:

1. GlobalPlatform proposes to issue a **TEE Restricted Security Evaluation Certificate**, which requires the agreement of the Vendor to prepare a joint **Risk Analysis Report** containing information for Users of the TEE Product;
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 TEE Users will receive reliable information derived from the TEE evaluation, which is meaningful to the risk assessment of their TEE services or deployments. GlobalPlatform Security Evaluation Secretariat 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 will issue the **TEE (Restricted) Security Evaluation Certificate** without delay upon edition of the **TEE (Restricted) Security Certification Report.** The certificate shall contain the TEE Security Certificate Number (TEESCN), a unique four-digit reference number identifying the TEE Product that has been evaluated and certified.

The management of the life-cycle of **TEE (Restricted) Security Evaluation Certificate** and the publication rules are described in section 3.4.

3.1.8 Product Identification

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

Upon evaluation request:

- Product name and version are required in the **Product Evaluation Request Form** for registering a TEE 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 TEE Security Target Template [TEE ST]):

  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 device (if applicable), the SoC, the firmware (ROM code), the boot code, the Trusted OS, the drivers, the pre-loaded TAs.

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. test boards, devices, 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 DTER and TER must provide the real Product name and version, as per the final Security Target;
- The DTER and TER must identify all the versions of TOE's components that have been audited/tested during the evaluation;
- The DTER and TER 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 **TEE (Restricted) Security Certification Report** and corresponding **TEE (Restricted) Certificate** shall include the real Product and TOE components identification, as per final Security target, TER and DTER;
- The **TEE (Restricted) Security Certification Report** and corresponding **TEE (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 Security Evaluation Secretariat together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform Security Evaluation Secretariat 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 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 Security Evaluation Secretariat together with the Exhibit B and Service Agreement as described in section 3.1.1.

GlobalPlatform Security Evaluation Secretariat 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 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 Certificate Management

3.4.1 Certificate

A **GlobalPlatform TEE Security Evaluation Certificate** confirms that the Product identified in the certificate has undergone security evaluation by an Accredited Laboratory against the TEE 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;
- [TEE PP] 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 TEE 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 Catalog 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.

3.4.2 Restricted Certificate

A **GlobalPlatform TEE Restricted Security Evaluation Certificate** confirms that the product identified in the Certificate has undergone security evaluation by an Accredited Laboratory against the TEE Protection Profile 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 TEE Restricted Security Evaluation Certificate** includes all information contained in an unrestricted certificate as defined in section 3.4.1 and the reference of the correspondent **Restricted Security Certification Report.**

A **GlobalPlatform TEE Restricted Security Certification Report** includes all information contained in an unrestricted certification report as defined in section 3.4.1 and the reference of the correspondent **Risk Analysis Report**.

3.4.3 Certification Validity

By default, a GlobalPlatform **TEE (Restricted) Security Evaluation Certificate** issued from a Full evaluation is valid for three (3) 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.

Nevertheless, GlobalPlatform reserves the right to withdraw a certificate upon certain circumstances, such as a significant change in the Attack Catalog.

3.4.4 Publication

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

Upon release of the **TEE (Restricted) Security Certification Report**, GlobalPlatform Security Evaluation Secretariat 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.

3.4.5 Security Monitoring

The GlobalPlatform Security Evaluation Secretariat through the TEE Attack Expert Working Group shall continuously monitor threats and security developments in TEE domain and update the Attack Catalog [TEE AP] to reflect the state-of-the-art.

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

4 Laboratory Accreditation

To perform TEE security evaluations under the GlobalPlatform TEE Security Evaluation Scheme, a laboratory must obtain and maintain GlobalPlatform accreditation. To do so, the laboratory shall apply for accreditation and successfully pass the corresponding audit. The audit tasks are undertaken by GlobalPlatform Qualified Auditors. Accreditation fees are due by the laboratory; payment shall be performed as stipulated by GlobalPlatform's policy.

Several types of audits may be required during a laboratory's relationship agreement with GlobalPlatform:

- Initial Accreditation Audit: This is the first audit that is required to become a GlobalPlatform Accredited Security Laboratory;
- Accreditation Renewal Audit: This audit is done before the expiration of an accreditation to extend the validity date;
- Interim Proficiency Audit: This audit is done upon GlobalPlatform request;
- Incremental Audit: This audit is done when the accredited laboratory moves to new premises.

GlobalPlatform reserves the right to suspend or revoke the accreditation status of a laboratory upon unsatisfactory renewal, incremental or interim audit. A laboratory whose accreditation has been suspended can recover the accreditation status upon a new successful audit of the type decided by GlobalPlatform.

4.1 Accreditation Types

4.1.1 Initial Accreditation Audit

When a laboratory initially requests GlobalPlatform accreditation, the laboratory supplies GlobalPlatform with documentation about the legal entity and an overview of its ability to meet GlobalPlatform accreditation requirements. GlobalPlatform reviews the documents supplied and, if the accreditation request is accepted, an accreditation audit is organized. Initial accreditation can only be granted upon successful audit.

The initial accreditation has a validity of two years provided the laboratory starts the first TEE Product evaluation within one year from the initial accreditation date.

4.1.2 Accreditation Renewal Audit

A GlobalPlatform Accredited Security Laboratory must be audited every two years to renew its GlobalPlatform accreditation. GlobalPlatform determines the requirements for the Accreditation Renewal Audit at the time of renewal. GlobalPlatform may select specific items for the auditor to cover. The audit must be completed before the expiration date of the laboratory's accreditation.

It is the responsibility of the laboratory to renew its accreditation before it expires. If a laboratory does not renew its accreditation, GlobalPlatform shall revoke its accreditation.

4.1.3 Interim Proficiency Audit

Under special circumstances, e.g. due to changes in the credentials, in the stakeholders or in the technical staff of the laboratory, or to comply with the decisions made upon the previous accreditation audit, GlobalPlatform may require an Interim Proficiency Audit. GlobalPlatform will inform the GlobalPlatform Accredited Security Laboratory about such decision, the date by which the audit must be completed, and the requirements that are in the scope of the audit (for instance, the scope of the audit upon a significant change in the technical staff should primarily include laboratory's testing capabilities).

If a laboratory does not complete the audit to the satisfaction of GlobalPlatform by the required date, GlobalPlatform may suspend or revoke the laboratory's accreditation.

4.1.4 Incremental Accreditation Audit

When a laboratory moves to new premises, an Incremental Accreditation Audit is required. The existing renewal date for the laboratory's accreditation does not change.

The requirements for an Incremental Accreditation Audit are determined by GlobalPlatform at the time of the audit.

If a laboratory does not complete the audit to the satisfaction of GlobalPlatform by the required date, GlobalPlatform may suspend or revoke the laboratory's accreditation.

4.2 Accreditation Process

The accreditation process is described in the following table. Note that all the agreements, forms, letters, and reports are in bold characters. In this process, the information that is provided by the laboratory is protected by a confidentiality agreement signed with GlobalPlatform.

Table 4-1: Accreditation Process

Entering the process	Laboratory	• Sends an accreditation request to GlobalPlatform Security Evaluation Secretariat including the following information (see **GlobalPlatform Laboratory Accreditation Request Form**): o Executive and financial summary; o Laboratory's facilities, background and experience; o Main contacts. • If the accreditation request is accepted: o Signs the **GlobalPlatform Security Laboratory Relationship Agreement**; o Formally accepts the audit proposal and proceeds with the payment of the accreditation fees as per GlobalPlatform financial conditions.
	GlobalPlatform Security Evaluation Secretariat	• Examines the accreditation request and, if necessary, requires additional information to the laboratory. • Decides to accept or reject the accreditation request[3] and informs the laboratory about the decision. • If the accreditation request is accepted, GlobalPlatform provides: o A **Letter of Registration** including the Registration Number to be used in all the communications with GlobalPlatform; o The **GlobalPlatform Security Laboratory Relationship Agreement** for signature; o The audit proposal including the scope, the auditor(s) names and the initial audit plan.
Audit	Laboratory	• Provides the auditors with information required in section 4.4 prior the audit (see GlobalPlatform Accreditation Guidelines and Audit Plan [TEE LAG]). • Hosts the on-site audit, presents technical topics and performs demonstrations as agreed in the audit plan. • Reviews the **Preliminary Audit Report** issued by GlobalPlatform Auditors after the audit. • If necessary, defines a **Corrective Action Plan** with deliverables and due dates to meet all GlobalPlatform requirements.
	GlobalPlatform Qualified Auditor	• Performs the audit against the accreditation requirements defined in section 4.3. • Writes the **Preliminary Audit Report** and provides it to the laboratory and GlobalPlatform Security Evaluation Secretariat.

[3] GlobalPlatform reserves the right, at its own discretion and without providing a detailed explanation, to deny a laboratory the right to proceed through the accreditation process.

		• Reviews the **Corrective Action Plan** defined by the laboratory, if applicable. • Writes the **Final Audit Report**, which includes the **Corrective Action Plan**, if applicable, and the accreditation recommendation, and provides it to GlobalPlatform Security Evaluation Secretariat.
	GlobalPlatform Security Evaluation Secretariat	• Monitors the accreditation audit.
Approval	GlobalPlatform Security Evaluation Secretariat	• Reviews the **Preliminary Audit Report** and provides feedback to the Qualified Auditor. • Reviews the **Final Audit Report** and determines whether the laboratory can be accredited and whether follow-up actions are required[4]. • Issues the **Final Audit Report** agreed with the Qualified Auditor(s). • If the decision is to grant accreditation without reserves: o Signs the **GlobalPlatform Security Laboratory Relationship Agreement**; o Issues an **Initial Letter of Accreditation** with a validity of one year; o Adds the laboratory to the list of Accredited Laboratories on the GlobalPlatform website. • If the decision is to grant provisional accreditation: o Signs the **GlobalPlatform Security Laboratory Relationship Agreement** with the laboratory; o Issues a provisional **Letter of Accreditation with conditions**, including the requirements for an **Interim Proficiency Audit** and a date by which it must be completed; o Adds the laboratory to the list of Accredited Laboratories on the GlobalPlatform website. • If the decision is to deny accreditation: o Notifies the laboratory about the decision.
	Laboratory	• Performs a TEE Product evaluation during the validity period of the **Initial Letter of Accreditation** or the **Initial Letter of Accreditation with conditions**.

The **Preliminary** and **Final Audit Reports** and any of its intermediate versions shall be protected against disclosure and unauthorized modification by their authors and recipients.

Nevertheless, GlobalPlatform may decide to communicate the **Final Audit Report** to partner organizations under MOU, upon authorization by the Laboratory.

[4] GlobalPlatform reserves the right to deny accreditation at its own discretion and without detailed explanation.

4.3 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.

4.3.1 General Requirements

4.3.1.1 GlobalPlatform Membership

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

[GR-02] The laboratory shall be a registered member of the GlobalPlatform TEE Security Laboratories and TEE Attack Experts Working Groups and shall comply with their participation rules.

4.3.1.2 Third-party Security Accreditations

[GR-03] The laboratory shall hold an ISO/IEC 17025 certificate issued by its national accreditation body that is valid at the date of audit.

a. Whether or not the technical scope of the ISO accreditation includes the TEE evaluation methodology as defined by GlobalPlatform, the laboratory shall perform such evaluations within the framework of processes and procedures under ISO accreditation.

[GR-04] The laboratory shall be accredited by at least one recognized security certification scheme such as Common Criteria, EMVCo or PCI.

4.3.2 Business Requirements

4.3.2.1 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 TEE evaluation activity unless permitted in writing by GlobalPlatform.

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

4.3.2.2 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.

4.3.2.3 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 the **GlobalPlatform Security Laboratory Relationship Agreement**.

4.3.2.4 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 TEE 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 **TEE Security Requirements**.

4.3.2.5 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 TEE Product(s) under evaluation.

[BR-12] The laboratory shall immediately notify the GlobalPlatform Security Evaluation Secretariat 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 TEE 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 TEE 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 TEE 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 TEE Security Evaluation.

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

4.3.2.6 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 TEE Product, without any further investigation and without any discrimination regarding pricing for complementary testing.

4.3.3 Organizational Requirements

4.3.3.1 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.

4.3.3.2 Personnel

[OR-04] The laboratory shall maintain a list of their qualified test personnel consisting of a description of their role in the organization, their qualifications, and their experience.

[OR-05] The laboratory shall have procedures to ensure a match between staff training and roles in the performance of GlobalPlatform TEE evaluation activities.

[OR-06] The laboratory shall maintain a file for each employee, which documents the employment history as permitted by law. For instance:

- Name and national identification number;
- Current photograph, updated at least every three years;
- Resume and job application;
- Level and title of formal education;
- Date of entry;
- Up-to-date track of:

    Signed document indicating that the employee has read and received a copy of the laboratory's policies and procedures;

    Trainings, especially those involving any GlobalPlatform testing process or GlobalPlatform-qualified test tools;

    Verification of aliases (if applicable);

- Check-out statement including the following items:

    Recovery of the employee's photo ID badge or access card, access keys, or passes and immediate deactivation of any access means;

    Ensure that the employee surrenders all property and documentation regarding GlobalPlatform security evaluations;

    Ensure that all computer and local area network access passwords are revoked.

4.3.3.3 Evaluation Facilities

[OR-07] The laboratory shall conduct all activities related to TEE Product evaluation and reporting within the audited laboratory's premises unless GlobalPlatform has granted written authorization to perform some well-identified activities at Vendor premises. In such a case, the laboratory shall register GlobalPlatform's authorization in the evaluation file.

4.3.4 Capability Requirements

4.3.4.1 Laboratory Experience and Expertise

[CR-01] The laboratory shall be able to demonstrate experience of at least three (3) years in security evaluation of IT products, which is relevant to the software and hardware testing of TEE Products as defined by GlobalPlatform.

[CR-02] The laboratory shall be able to demonstrate expertise in the areas that are relevant to TEE Products' evaluation as defined by GlobalPlatform, including TEE specifications, System-on-Chip architectures, (micro-)kernels, as well as related software and hardware attack techniques.

[CR-03] The laboratory shall define and implement a process for monitoring the public TEE-related vulnerabilities.

[CR-04] The laboratory shall define and regularly update a training program about TEE technology and related testing technics aimed at all the personnel that is involved in TEE evaluations.

[CR-05] The laboratory shall notify to GlobalPlatform Security Evaluation Secretariat in writing and without delay the departure of lead evaluator(s) or any change in the organization that may impact the global level of expertise of the laboratory.

4.3.4.2 Personnel Experience and Expertise

[CR-06] The laboratory shall ensure that the personnel performing GlobalPlatform TEE evaluations has appropriate academic background, e.g. in areas such as Computer Science, Mathematics, Cryptography, Microelectronics, sufficient TEE knowledge and skills to apply the TEE evaluation methodology and to operate the equipment of the laboratory.

[CR-07] The laboratory shall appoint one or several TEE lead evaluator(s), with at least three (3) years of experience in TEE or similar security evaluations, to support the laboratory's technical manager with regards to GlobalPlatform TEE evaluations and to the maintenance of the laboratory's TEE expertise.

[CR-08] The laboratory shall ensure that the TEE lead evaluator(s) have received the latest GlobalPlatform TEE training and that processes are in place to share such knowledge with the entire TEE technical personnel.

4.3.4.3 Test Methodology and Equipment

[CR-09] The laboratory shall define operational methods and procedures to apply GlobalPlatform TEE evaluation methodology in a reproducible and harmonized way across evaluations and evaluators.

[CR-10] The laboratory shall own or have access to the hardware and software equipment that is necessary to perform the TEE evaluations, including source code review, security functional testing and penetration testing, as defined by GlobalPlatform.

[CR-11] The laboratory shall demonstrate the capability to perform automated security functional testing of GlobalPlatform compliant TEE Products, compliant with latest versions of GlobalPlatform security test suites.

[CR-12] The laboratory shall ensure that maintenance of hardware test equipment is authorized before the effective maintenance activities begin. The maintenance activities shall be performed under the control and authorization of the laboratory's management, following a documented procedure which includes signing the equipment over to maintenance and signing the equipment back to production.

[CR-13] The laboratory shall ensure that software test equipment is protected from unauthorized modification. The update of such equipment shall be performed under continuous supervision of the laboratory's management, following a documented procedure which includes signing the equipment over to maintenance and signing the equipment back to production.

4.3.5 Security Requirements

4.3.5.1 Physical Security Policy

[SR-01] The laboratory shall maintain and comply with a physical security policy that addresses, at a minimum, the following aspects:

a. Physical security layer (e.g. fence, alarm system, CCTV);

b. Security controls (e.g. guards, badge access control);

c. Reaction upon incident detection;

d. Equipment used to enforce security (e.g. safe, safety lock, network physical security);

e. Delivery procedures (physical goods);

f. Access policy to laboratory's premises, including employees, contractors, trainees and visitors.

4.3.5.2 Logical Security Policy

[SR-02] The laboratory shall maintain and comply with a logical security policy that addresses, at a minimum, the following aspects:

a. Network segregation (firewalls and servers);

b. Network access control (local and remote);

c. Network intrusion detection and reaction policy;

d. Information management and protection policy;

e. Desktop policy;

f. Backup systems.

4.3.5.3 Physical Layout

[SR-03] The laboratory shall demonstrate the sufficiency of the access policy and security controls to prevent unauthorized people from entering the laboratory's premises.

4.3.5.4 Evaluation Areas

[SR-04] The laboratory shall restrict the access to the evaluation area to authorized personnel. Areas in the laboratory facilities in which products, components, or data are tested or stored are called *evaluation areas* for the purpose of this document.

[SR-05] The laboratory shall restrict the access to test equipment to authorized personnel. This includes physical or network access.

4.3.5.5 Networks

[SR-06] The laboratory shall ensure that all the systems that are used to handle test data or constituent parts of test data are accessible from internal network(s) that are isolated from the outside and exclusively accessible to authorized personnel from authorized terminals.

[SR-07] The laboratory shall ensure that computers and servers used to store sensitive information (evaluation reports, TEE Product data, etc.) are disconnected from any network – external or internal - which does not enforce exclusive access by authorized personnel and terminals.

[SR-08] The laboratory shall ensure that whenever non-dedicated networks are used then sufficient controls are in place to protect the integrity and the confidentiality of the sensitive data. These controls include, for instance, the use of appropriate firewalls and routers.

[SR-09] The laboratory shall ensure that networks linking the laboratory to third-parties for the transfer of customer and laboratory information are separate and isolated from the test system.

[SR-10] The laboratory shall ensure that networks that link different laboratory premises implement suitable and sufficient controls to protect sensitive data, e.g. systematic encryption, to achieve the same security level as within a single site.

[SR-11] The laboratory shall define and comply with a secure method of transferring customer data to test equipment that does not introduce security risks or vulnerabilities.

4.3.5.6 Storage and Backup

[SR-12] The laboratory shall demonstrate that it has sufficient secure storage space to provide adequate protection for all on-going work. Additional secure storage shall be provided for all materials retained by the laboratory after evaluation has been completed.

[SR-13] The laboratory shall ensure that all back-up processes and storage means are managed according to industry standards for recovery purposes.

4.3.5.7 Classified Materials and Information

[SR-14] The laboratory shall handle classified test samples, documents, and specifications with particular care and keep them within the audited premises such that they are accessible only to authorized personnel.

[SR-15] The laboratory shall control and store securely all classified test materials and information, e.g. samples, documents, and specifications, received from GlobalPlatform or a product vendor, whether in physical or electronic format.

[SR-16] The laboratory shall store classified test material in secure containers, where unauthorized access is prevented by appropriate measures (e.g. alarms, surveillance, and sufficient physical protection).

[SR-17] The laboratory shall ensure that disclosure of GlobalPlatform or TEE Product vendor classified materials, data or documents to third-parties is authorized in writing by an officer of the company that owns the materials, data or documents to be delivered. Receipt of such kind of items must be acknowledged by signature of the company’s official representative.

a. In the context of a GlobalPlatform evaluation, when a product vendor grants permission to the laboratory to disclose classified product information to GlobalPlatform, this information shall be transmitted to GlobalPlatform Security Secretariat exclusively.

4.3.5.8 Evaluation Materials and Reports

[SR-18] The laboratory shall store all evaluation reports and related materials securely. If reports are stored electronically, they must be in an industry-recognized protected form.

[SR-19] The laboratory shall store evaluation materials including test samples and all reports and logs from the evaluations in paper or electronic form for a period of six (6) years following the expiration date of the certificate.

[SR-20] The laboratory shall deliver physical goods related to the evaluation, i.e. evaluation reports and related classified documents that are issued in paper or evaluation samples, in a tamper-evident package identified by a unique number.

[SR-21] The laboratory shall deliver to GlobalPlatform Security Secretariat and product vendor electronic evaluation reports and related classified documents in encrypted format using asymmetric cryptography or using an equivalent protection method that is agreed with the recipient(s).

4.4 Audit Requirements

The accreditation audit is split in two parts as described below: preliminary documentation audit, based on written evidences, and site visit.

4.4.1 Documentation Audit

Prior the visit to the laboratory's premises, the laboratory shall provide to the GlobalPlatform Qualified Auditor(s) the following:

- Written information that supports the laboratory requirements defined in section 4.3.
- List of relevant documents that will be available on-site.

The information shall consist of, for instance:

- Official documents with unique reference, version number and date of issuance, in pdf format;
- Dated samples of log books and files, in pdf or image format;
- Dated screen shoots of tools, in pdf or image format.

The accreditation guidelines [TEE LAG] define the minimum information that is required from the laboratory.

The laboratory may provide to the GlobalPlatform Qualified Auditor(s) copies of the Audit Reports issued by third-parties organizations, to allow some reuse of results at the discretion of GlobalPlatform Qualified Auditor(s).

GlobalPlatform Qualified Auditor(s) have the right to require complementary information anytime from the start of the accreditation process until the end of the reporting phase. In particular, the Auditor(s) may require access to specific documentation during the site visit.

4.4.2 Site Visit

GlobalPlatform requires the Qualified Auditor(s) to conduct a visit at each site for which the laboratory is seeking an accreditation. The main objectives of the site visit are to:

- Observe the physical environment of the laboratory and the security measures that are implemented;
- Verify the laboratory's quality assurance procedures related to the ISO/IEC 17025:2005 [ISO 17025] certificate and their validity and application in the framework of GlobalPlatform TEE security evaluations;
- Verify that laboratory documentation and actual laboratory implementation are in agreement;
- Verify the laboratory's technical expertise related to TEE, through technical presentations, demonstrations and discussions with the evaluators;
- Observe the test equipment that is available within the laboratory.

Special attention will be paid to the laboratory's methodology and procedures for TEE-related testing, which provides the cornerstone of the laboratory role, and to the evidence of the laboratory experience in the field.

The agenda of the site visit(s) shall be agreed between GlobalPlatform Qualified Auditor(s) and the laboratory during the documentation audit phase, in particular the technical presentations and demonstrations.

4.4.3 Demonstration of Testing Capabilities

GlobalPlatform may require a demonstration of the laboratory's actual testing capabilities through witnessing the laboratory's testing of a TEE Product or through pilot testing.

Pilot testing is defined as the laboratory's performing evaluation on a previously certified TEE Product or on a simulation product and providing an evaluation report to the GlobalPlatform Qualified Auditor for review. The choice of the subject of such pilot testing and the extent of the witnessing, either full or partial rests with GlobalPlatform.

The format and presentation of assurance evidence should be an essential part of this exercise, in addition to the demonstration of the testing capabilities. Results are expected to be prepared in accordance with ISO standards and GlobalPlatform requirements. Accreditation Termination

At any time, a **Security Laboratory's Relationship Agreement** between GlobalPlatform and an Accredited laboratory may be:

- terminated upon laboratory's decision;
- suspended or revoked upon GlobalPlatform's decision.

4.5 Termination Process

4.5.1 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.

4.5.2 Suspension by GlobalPlatform

GlobalPlatform has the right to suspend at any time a laboratory's accreditation:

- Based on the results of an **Audit Report**;
- Due to the non-conformance with GlobalPlatform's requirements;
- If a laboratory fails to complete an **Incremental Audit** or **Interim Proficiency Audit** to the satisfaction of GlobalPlatform by the required date.

Upon suspension, GlobalPlatform 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.

4.5.3 Revocation by GlobalPlatform

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

- Based upon the results of an **Audit Report**;
- Due to non-conformance with GlobalPlatform's requirements;
- If a laboratory has not performed testing of TEE 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.

Annex A TEE Parts Certification

This annex introduces the extension of GlobalPlatform TEE Certification Scheme to TEE Parts. The goal is to facilitate the certification of TEE Products, through the reuse of the intermediate certificates obtained for some TEE Parts by their own Vendors.

A TEE Part stands for a set of hardware, firmware and/or software which provides TEE-related security functionality and has well-defined physical and logical boundary (interfaces). Typical examples of TEE Parts are:

- SoC with ROM code;
- Trusted OS (potentially with boot code).

The main advantage of certification by-parts is indeed the possibility to run hardware-only and software-only security evaluations in parallel, on behalf of their respective Vendors. In the end, their integration must be evaluated to achieve full TEE certification. Although nothing prevents such reuse when the same laboratory evaluates both the TEE Parts and the complete TEE Product, the GlobalPlatform TEE certification by-parts allows to reuse certified TEE Parts, which have been evaluated by different laboratories, within a TEE evaluation by any other laboratory.

However, a software-only or hardware-only Protection Profile is not required nor suitable since there are lots of ways of implementing the TEE. As a counterpart, the Vendor must provide a Security Target that is specific to the TEE Part, i.e. for which there is no predefined content: the ST shall describe the TEE Part, its security functionality and interfaces and shall provide a rationale against the [TEE PP]. By definition, compliance with the [TEE PP] is not achievable since the TEE Part is a strictly included in a TEE Product; such rationale is necessary to confirm the relevance of the certification in the GlobalPlatform TEE certification scheme and to provide guidance for the reuse of the certified TEE Part in a TEE Product evaluation. A successful evaluation implies the validation of the TEE Part Security Target by the laboratory.

The principles of a TEE Part evaluation are the same as for TEE Products. The laboratory:

- performs vulnerability analysis of the TEE Part through documentation and source code review, runs automated functional tests if applicable;
- defines a test plan to cover the security claims of the Security Target and the relevant attack methods defined in the Attack Catalog for such kind of Part;
- reports the evaluation results in DTER/TER, which contains a specific chapter about the usage of the results in a full TEE Product evaluation.

The principles of a TEE Part certification are the same as for TEE Products. GlobalPlatform SES:

- pre-approves the TEE Part Security Target upon evaluation request;
- reviews the TER (and DTER if needed) together with the final Security Target;
- writes the TEE Part Security Certification Report;
- issues the TEE Part Security Evaluation Certificate, with 3-year by default validity.

GlobalPlatform will publish such Certificates and corresponding Certification Reports in a separate list, following the same rules as for TEE Products (see section 3.4.4).

A TEE Product evaluation may reuse certified TEE Parts, as defined in section 2.4.2. The Vendor of the TEE Product must provide to the laboratory the TEE Security Target, as usual, and a TEE Integration document which explains how the different Parts are assembled together and to other parts to build the TEE Product. Moreover, the laboratory must have access to the Certification Report(s) of the TEE Part(s) and may require the corresponding Security Target(s) and the DTER/TERs. The disclosure of such evidences by the Vendor(s) of the TEE Part(s) to theirs partners is out of scope of GlobalPlatform scheme.

GlobalPlatform SES will validate the reuse of certified TEE Part(s) upon the registration of the TEE Product evaluation. In such case, the **(Restricted) Security Certification Report** of the TEE Product shall reference all the underlying TEE Part(s) certificates.

The revocation of a **TEE Part Security Evaluation Certificate** will entail the analysis of all the relying **TEE Security Evaluation Certificates**, which may lead to their confirmation or revocation in a case-by-case basis. GlobalPlatform reserves the right to make such decision at its own discretion.