GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform

TEE Certification Process

Version 1.0

Public Release

July 2015

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 defines the processes associated with the GlobalPlatform TEE Certification Scheme, including management of the Security Requirements, the process to apply for laboratory accreditation, the process to apply for product certification, and management of the certificates.

The GlobalPlatform TEE Certification Scheme is the organization under which laboratories are accredited, products are evaluated, and **TEE Security Evaluation Certificates** are issued. The GlobalPlatform TEE Certification Scheme is under GlobalPlatform responsibility and is managed by the GlobalPlatform Security Evaluation Secretariat. It involves TEE Vendors, GlobalPlatform Accredited Security Laboratories, and TEE Users. It applies to any device implementing GlobalPlatform TEE specifications.

Please check the TEE Certification webpage at http://www.globalplatform.org/TEECertification.asp for the latest applicable documents and fee structure. In case of differences, the website published version of documents supersedes the information in this document.

1.1 Audience

This document is intended primarily for vendors of TEE or TEE-enabled devices and for 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

Table 1-1: Normative References

Standard / Specification	Description	Ref
GPD_SPE_021	GlobalPlatform Device Committee TEE Protection Profile (PP-base and PP-modules)	[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	[TEE EM]
GPD_TEN_045	GlobalPlatform TEE Security Target Template	[TEE ST]
GPD_SPE_050	GlobalPlatform TEE Common Automated Tests	[TEE CAT]
ISO/IEC 17025	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 Digital Letter of Approval [to be published]	[DLOA]

1.4 Terminology and Definitions

Table 1-3: Terminology and Definitions

Term	Definition
GlobalPlatform Accredited Security Laboratory	A laboratory and/or 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 for security evaluation laboratories.
GlobalPlatform Security Laboratory Relationship Agreement	Agreement between GlobalPlatform and the laboratory.
Product	A TEE Product, which includes any 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 given product by a Product Vendor, through the Evaluation Process.
Product Registration Number	A unique number identifying the TEE, assigned at the start of the evaluation process.
Product Vendor	An entity submitting a product for security evaluation assessment under the Evaluation Process, including but not limited to Vendor.
Restricted Certificate	The written, formal recognition and acknowledgement of restricted certification of a Product under the Evaluation Process and provided by GP to a Product Vendor for a given Product, where a Product is found to have a vulnerability under the Evaluation Process.
Risk Analysis Report	The report, prepared jointly by GP and a Product Vendor in the event the Product Vendor elects not to remedy vulnerabilities identified as part of the Evaluation Process, and containing information for parties intending to use the Product Vendor's Product.
Security Requirements	Collectively, the most recent version (unless GlobalPlatform specifies and 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 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.
TEE Security Certificate Number	A unique four-digit reference number that applies only to the exact product configuration described in the GlobalPlatform TEE Security Evaluation Certificate.

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
OS	Operating System
PP	Protection Profile
REE	Rich Execution Environment
SFR	Security Functional Requirement
SoC	System-on-Chip
ST	Security Target
TA	Trusted Applications
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	Public Release

2 Overview

This document describes the processes associated with the GlobalPlatform TEE Certification Scheme. The GlobalPlatform TEE Certification Scheme consists of a set of requirements and processes that apply to TEE products. GlobalPlatform is the owner of the scheme and acts as the certification entity for all approvals relating to the security of the product embedding a TEE. The GlobalPlatform Security Evaluation Secretariat is the body that operates the scheme. The objective of the GlobalPlatform Certification Process is to ensure that TEE products comply with GlobalPlatform **TEE Security Requirements**.

The GlobalPlatform TEE Certification Process includes the following activities:

- Scheme definition and maintenance
- Laboratory accreditation
- TEE security evaluation management
- Certificate issuance, registration, and management

GlobalPlatform acts as a certification entity for approvals relating to the security of TEE, is responsible for overseeing the GlobalPlatform TEE Certification Process, and maintains the **TEE Security Requirements**, which is the complete set of documents that defines the evaluation work. The **TEE Security Requirements** serve as guidance for TEE Vendors when developing the product, and for GlobalPlatform Accredited Security Laboratories while performing TEE Security Evaluations. The GlobalPlatform Security Evaluation Secretariat is responsible for administering the GlobalPlatform TEE Certification Process.

GlobalPlatform does not, however, guarantee or provide any warranties for any TEE Vendor's products, and the GlobalPlatform TEE Certification Process does not relieve users from the responsibility to undertake their own investigations to ensure the security or fitness for purpose of any products. No implementation can be 100% secure, but the GlobalPlatform TEE Certification Process provides TEE Users with additional information to assist in their risk analysis with TEE Vendors.

2.1 Product Scope

The GlobalPlatform TEE Certification Process evaluates the security features of TEE products.

A TEE Product includes any device or SoC embedding a TEE. The precise scope of evaluation is defined in the TEE Protection Profile [TEE PP], it includes hardware and software security features, more precisely the SoC, the Trusted OS, and communication with the Rich Execution Environment (REE), but it does not include the Trusted Applications (TA) or the REE when the evaluation is performed on a device.

2.2 Actors

The following actors are referred to in this document:

- GlobalPlatform Security Evaluation Secretariat
- GlobalPlatform Qualified Auditors
- GlobalPlatform Accredited Security Laboratories
- TEE Vendors
- TEE Users

GlobalPlatform Security Evaluation Secretariat

GlobalPlatform through the GlobalPlatform Security Evaluation Secretariat, is the owner of the GlobalPlatform TEE Certification Scheme.

It is responsible for:

- GlobalPlatform TEE Certification Process definition and maintenance, this document
- GlobalPlatform TEE Security Requirements maintenance (Chapter 3)
- Laboratory accreditation and maintenance (Chapter 4)
- Vendor application request validation (Chapter 5)
- Certificate delivery, registration, and publication (section 5.5)

GlobalPlatform Qualified Auditors

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

GlobalPlatform Accredited Security Laboratories

GlobalPlatform Accredited Security Laboratories are accredited by GlobalPlatform and perform TEE Security Evaluations. GlobalPlatform accreditation is described in Chapter 4, and involves a **GlobalPlatform Security Laboratory Relationship Agreement** to be signed with GlobalPlatform describing 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:

- Applying for and renewing their accreditation.
- Evaluating product(s) from TEE Vendors following the TEE Security Requirements and especially the TEE Evaluation Methodology [TEE EM].
- Creating a **Detailed TEE Evaluation Report (DTER)**
- Creating a **TEE Evaluation Report (TER)** that is also transmitted to the TEE Vendor.

GlobalPlatform Accredited Security Laboratories must be GlobalPlatform members and must contribute to at least the following two Device Committee Working Groups: TEE Attack Experts WG and Security Laboratories WG.

TEE Vendors

TEE Vendors apply for TEE Security Evaluation. Application includes a **Security Evaluation Agreement** to be signed with GlobalPlatform setting the GlobalPlatform evaluation fees and describing the obligations of the TEE Vendor in terms of communication.

TEE Vendors are responsible for:

- Providing a completed **Product Evaluation Request Form**
- Contracting with a GlobalPlatform Accredited Security Laboratory
- Providing the information and material listed in the TEE Evaluation Methodology [TEE EM] to the GlobalPlatform Accredited Security Laboratory
- Participating in communication related to the GlobalPlatform Security Evaluation Process with the GlobalPlatform TEE Security Evaluation Secretariat

TEE Users

“TEE Users” represents any actor that relies on TEE security features: typically service providers. When relying on a certified TEE, it is the TEE User’s responsibility to check:

- Type and validity of the **TEE Security Evaluation Certificate**
- TEE Perimeter
- Limitations in case of a restricted **TEE Security Evaluation Certificate**

A subsequent version of this document will identify certificate related information that can be found in the Digital Letter of Approval (DLOA), as specified in GlobalPlatform Digital Letter of Approval [DLOA], currently under development.

2.3 Principle of the TEE Certification Process

2.3.1 Scope of the Security Evaluation

The GlobalPlatform TEE Certification Process is based on a complete set of published GlobalPlatform specifications, **TEE Security Requirements**, which serve as the security requirements for product vendors.

The process establishes that product vendors are responsible for security evaluation and demonstration of sufficiency within the **TEE Security Requirements**.

This process benefits both to TEE Users and product vendors by defining a flexible, state of the art, common security evaluation methodology that is recognized by all GlobalPlatform participants. The GlobalPlatform TEE Certification Process strives for the appropriate level of assurance for TEE products regarding the market and defined in the Protection Profile [TEE PP] as AVA_TEE.2 level.

The evaluation methodology [TEE EM] has been designed to enable GlobalPlatform Accredited Security Laboratories to perform the evaluation in three (3) months when all information is accessible in a straightforward manner.

The evaluation methodology strives to achieve a balance between automated Black Box and White Box testing. This is achieved by carrying out a security analysis that considers all viable attacks on a product, and derives a set of penetration tests based on individual product characteristics.

The GlobalPlatform TEE Attack Experts Working Group will maintain the state of the art methodology, which shall constantly update the attack catalogue and trigger update to [TEE PP] when necessary.

Certificates will be issued through the GlobalPlatform Security Evaluation Secretariat.

2.3.2 Reuse of Evaluation Work Done in Other Schemes

GlobalPlatform will reuse as much as possible work done in another context such as:

- Security evaluation work using the relevant GlobalPlatform **TEE Security Requirements** and performed under a formal evaluation scheme (e.g. Common Criteria)
- Site audits

The inputs must be clearly and uniquely identified in the **Product Evaluation Request Form**.

2.3.3 Certificates

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

In case a potential vulnerability is found, a GlobalPlatform **Restricted Security Evaluation Certificate** may be issued. If this happens, the product vendor is made fully aware of the details of any such problems, and GlobalPlatform will work with the product vendor to achieve two things:

- The vulnerability is adequately communicated by the product vendor to TEE Users to enable them to assess their own risks.
- A plan is put in place by the product vendor to introduce a revised product that reduces the vulnerability. GlobalPlatform also reserves the right to withdraw or not to issue a GlobalPlatform **Security Evaluation Certificate** or a GlobalPlatform **Restricted Security Evaluation Certificate** when the product does not offer sufficient protection.

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

Certified products are placed on the GlobalPlatform Evaluated Products List. When certificates are not valid anymore, products are removed from the list.

Validity is given for three years unless stated otherwise (see section 5.5.3).

2.3.4 Certificate Recognition

GlobalPlatform is finalizing the conditions under which Common Criteria Certificates of product based on the GlobalPlatform TEE Protection Profile [TEE PP] could be reused (typically certificates issued by a Certification Body that participates in the TEE Attack Experts Working Group and mandates [TEE PP], and certified against a superset of the GlobalPlatform list of attack).

2.3.5 Risk Management

Most of the TEE Users are in a risk management business that has to constantly monitor vulnerabilities and threats. When a product vendor sells a product, that product vendor should be able to explain the testing that has been carried out in order to verify conformance with GlobalPlatform Security Requirements.

The level of testing reflects the state of the art attack potential. Consequently, the introduction of new products should offer a higher level of protection against the latest threats. However, no testing can anticipate all potential future attacks.

TEE Users should constantly bear in mind that there is no perfect security and that security level of a given product is likely to decrease over time. An attack made with sufficient effort (in terms of skills, equipment, and time) will always succeed in compromising those assets. The GlobalPlatform TEE Certification Process aims at identifying vulnerabilities in these terms to fit into a formal risk analysis of a system. A secure system must implement defenses at all levels, and TEE Users should develop separate strategies for prevention, detection, and recovery.

There are essentially two motivations for an attacker: publicity and benefits. Incident management procedures should be in place for each, and appropriate security measures should be taken to limit the likely benefits that an attacker may achieve with their efforts.

In the event that a TEE product only receives a GlobalPlatform **Restricted Security Evaluation Certificate**, the product vendor should be in a position to explain the reasons, and 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 other security measures.

2.4 Processes

The following processes support the evaluation:

- GlobalPlatform TEE Certification Scheme definition and maintenance done by the GlobalPlatform Security Evaluation Secretariat and GlobalPlatform groups
- Laboratory accreditation done by the GlobalPlatform Security Evaluation Secretariat and GlobalPlatform Qualified Auditors
- Evaluation of the TEE product done by Global Platform Accredited Security Laboratories
- Certification of the TEE product done by the GlobalPlatform Security Evaluation Secretariat

3 Security Requirements

The GlobalPlatform TEE Certification Process reflects a partnership with TEE Vendors, and the entire TEE ecosystem and seeks to minimize the cost and time spent in performing evaluation work and, where possible, avoid the duplication of effort. By leveraging the modular evaluation methodology, evaluations that are based on a core family of devices can use delta evaluations to manage product migration. Associated design is evaluated once, and the paperwork overhead is reduced.

The GlobalPlatform TEE Certification Scheme is defined by this document and three (3) other main documents that together form the **TEE Security Requirements**:

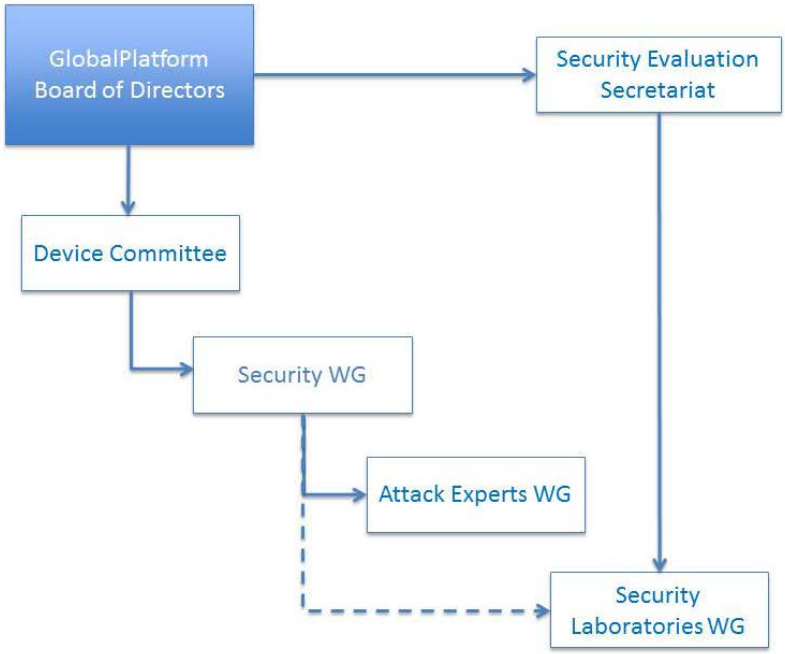
- TEE Protection Profile [TEE PP]
- TEE Evaluation Methodology [TEE EM]
- The Attack Catalog [TEE AP]

These documents are managed by the following entities:

- The Security Evaluation Secretariat is in charge of defining the process, supervising the evaluation, managing laboratory accreditation, issuing and publishing the security certificates, and managing communication about the GlobalPlatform TEE Certification Scheme.
- The TEE Security Working Group is in charge of defining and maintaining [TEE AP]. It also manages the Protection Profile certification in the Common Criteria scheme.
- The TEE Security Laboratories Working Group is in charge of defining and maintaining [TEE EM].
- The TEE Attack Experts Working Group is in charge of defining and maintaining [TEE AP].

Figure 3-1 illustrates how these Working Groups are related in the GlobalPlatform organization.

Figure 3-1: GlobalPlatform Organization for TEE Certification



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

3.1 Certification Process Document

Owner: GlobalPlatform Security Evaluation Secretariat

Content: Overall process

Audience: Laboratories, TEE Vendors, TEE Users

Distribution: The latest GlobalPlatform TEE Certification Process document shall be available under the TEE Certification Scheme page of www.globalplatform.org.

3.2 Protection Profile

Owner: GlobalPlatform TEE Security Working Group

Content: The Protection Profile [TEE PP] consists of a set of documents defined as per of the Common Criteria rules, describing the Security Requirements for the TEE in a modular way. It contains an extract of the Attack Catalog [TEE AP] and the reference to the applicable version of [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

Depending on the nature of the update, it can result in the addition of a module or in an update to the PP Core Configuration.

Protection Profile Approval/Certification

- The initial version of the 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 on the Device Specification page of www.globalplatform.org.

3.3 Evaluation Methodology

Owner: GlobalPlatform Security Laboratories Working Group

Content: This document describes the process and requirements for vendors and GlobalPlatform Accredited Security Laboratories to perform TEE evaluation conformant with the security functional requirements and robustness level defined in GlobalPlatform TEE Protection Profile [TEE PP].

Updates of the Evaluation methodology may be triggered by:

- Feedback from the field
- Modification of the scope/duration, acceptable form factors, automated test list
- Reuse of results from other evaluation schemes
- Protection Profile update
- TEE specification update
- Attack Catalog [TEE AP] update
- TEE Protection Profile [TEE PP] update

Audience: Laboratories and vendors

Distribution: The applicable Evaluation methodology shall be available on the GlobalPlatform Member Only Documentation page of https://members.globalplatform.org.

3.4 Attack Catalog

Owner: GlobalPlatform TEE Attack Experts Working Group

Content: List of attacks that have to be considered while performing a TEE evaluation. The expected update frequency is every six (6) months.

Updates of the Attack Catalog document may be triggered by:

- New attacks coming from GlobalPlatform Accredited Security Laboratory findings or from the field
- Protection Profile [TEE PP] scope evolution

Audience: Laboratories

Distribution: The Attack Catalog is restricted to GlobalPlatform TEE Attack Experts Working Group members, which includes the GlobalPlatform Accredited Security Laboratories.

GlobalPlatform manages communication between the TEE Attack Experts Working Group and external entities.

4 Laboratory Accreditation

To perform TEE security evaluation 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 appropriate audits. The audit tasks are undertaken by GlobalPlatform Qualified Auditors. Payment of Auditors' fees is the responsibility of the laboratory requesting GlobalPlatform's accreditation.

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

- Initial Accreditation Audit: This audit is required to initially become a GlobalPlatform Accredited Security Laboratory.
- Accreditation Renewal Audit: This audit is done before the expiration of a valid audit to extend the validity date.
- Interim Proficiency Audit: This audit is done upon request of GlobalPlatform.

4.1 Accreditation Types

4.1.1 Initial Accreditation

When a laboratory initially requests GlobalPlatform accreditation, the laboratory supplies GlobalPlatform with documentation about the laboratory, which includes an overview of its abilities to meet GlobalPlatform accreditation requirements. Once GlobalPlatform has reviewed the documents supplied and has accepted the laboratory for potential accreditation, a full accreditation audit is required. The initial accreditation is completed once an evaluation has been performed.

4.1.2 Accreditation Renewal

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

At any time, at the discretion of GlobalPlatform, an Interim Proficiency Audit may be required. GlobalPlatform will inform the GlobalPlatform Accredited Security Laboratory:

- that an Interim Proficiency Audit must be performed and the date by which the audit must be completed,
- of the audit requirements (which will be based upon the issue identified).

The scope of the audit will primarily include a laboratory's testing procedures and capabilities.

If a laboratory does not complete the audit to the satisfaction of GlobalPlatform by the required date, GlobalPlatform may suspend or revoke its 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 from the laboratory is covered by confidentiality agreements with GlobalPlatform Security Evaluation Secretariat and with Qualified Auditors.

Table 4-1: Accreditation Process

Entering the process	Laboratory	• Sends request to GlobalPlatform at teecertification@globalplatform.org to begin the accreditation process; the request should include the following: o Executive and financial summary o Technical expertise summary, including experience with TEE Specifications o Laboratory background o Accreditation from other schemes o **GlobalPlatform Security Laboratory Accreditation Request form**
	GlobalPlatform Security Evaluation Secretariat	• Evaluates whether the laboratory qualifies to be accepted as a potential GlobalPlatform Accredited Security Laboratory • Informs laboratory whether it may proceed with accreditation[1] • Provides laboratory with: o The **GlobalPlatform Security Laboratory Relationship Agreement** o A **Letter of Registration** including a Registration Number, to be used on all communication and reports sent to GlobalPlatform o The scope of the audit
Audit	Laboratory	• According to the scope of the audit, the laboratory selects auditors from the list of GlobalPlatform Qualified Auditors and makes financial and legal arrangements with the auditors for the laboratory to be audited. • Signs the **GlobalPlatform Security Laboratory Relationship Agreement**. • Provides the auditors with information to meet audit requirement defined in section 4.4.
	GlobalPlatform Qualified Auditor	• Performs audit in accordance with [ISO 17025]. • Ensures laboratory meets all requirements detailed in section 4.3 and section 4.4. • Ensures expert performing evaluation are well trained and clearly designated • Audits the laboratory's testing capabilities and provides findings to the laboratory. • If a **Corrective Action Plan** (as described in section 4.4.5) is NOT necessary, provides **Audit Report** to GlobalPlatform.

[1] 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.

Audit	Laboratory	If a **Corrective Action Plan** is necessary: • Defines the **Corrective Action Plan** with deliverables and due dates to meet all GlobalPlatform requirements • Provides **Corrective Action Plan** to GlobalPlatform Qualified Auditor
	GlobalPlatform Qualified Auditor	If a **Corrective Action Plan** is necessary: • Reviews and validates the **Corrective Action Plan** defined by the laboratory • Provides a copy of the **Corrective Action Plan** with its **Audit Report** to GlobalPlatform
Approval	GlobalPlatform Security Evaluation Secretariat	• Reviews **Audit Report** (and **Corrective Action Plan**, if any) and determines whether the laboratory may be accredited or whether follow-up action is required[2] • If the Audit Report is acceptable to GlobalPlatform: o Signs the **GlobalPlatform Security Laboratory Relationship Agreement** with the laboratory. o Sends the laboratory 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 Audit Report is acceptable, but action items are required from the laboratory, GlobalPlatform may grant accreditation on a provisional basis, as follows: o Signs the **GlobalPlatform Security Laboratory Relationship Agreement** with the laboratory. o Sends the laboratory 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.
	Laboratory	Performs an actual evaluation during the validity period of the **Initial Letter of Accreditation** or the **Letter of Accreditation with conditions**.

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

4.3 Laboratory Requirements

This section identifies the business, security, administrative, and technical requirements that a laboratory must meet in order to obtain and maintain GlobalPlatform accreditation.

4.3.1 GlobalPlatform Requirements

- GlobalPlatform membership and participation
  - Be a GlobalPlatform full member or Device Committee participating member in good standing.
  - Actively participate in the Security Laboratories WG and TEE Attack Experts Working Groups.
- The following accreditation are required:
  - A valid [ISO 17025] certificate is mandatory. If the scope of the [ISO 17025] certificate does not include the TEE Security Evaluation perimeter, the audit will check that TEE Security Evaluation procedures comply with [ISO 17025] standard.
- The following expertise is required:
  - Security evaluation processes through accreditation by a recognized certification scheme such as Common Criteria, EMVCo, or PCI
  - Demonstrable experience of at least three (3) years in security evaluations of similar products with software & hardware security testing
  - TEE training (the employee performing the evaluation test should be trained with the latest version of the GlobalPlatform training)
  - Demonstrable capability including tools and infrastructure for the test coverage required as defined in [TEE EM] and [TEE CAT]

4.3.2 Business Requirements

This section describes the overall business requirements which a laboratory must meet.

- Financial
  - The laboratory must conduct business in a manner that is consistent with the highest ethical standards and with practices that minimize risk. The laboratory must be subject to a due diligence review, with the primary focus of identifying and mitigating potential financial and goodwill risks.
  - The laboratory must have a sound financial basis and be a part of a stable organization.
  - The laboratory must adhere to ethical business standards and practices.
  - The laboratory must have no financial dependencies on any product vendor for which testing is being performed other than the product vendor's payment for the service provided.
  - The laboratory must have no financial dependencies on any GlobalPlatform member with regards to performance of any GlobalPlatform activity unless permitted in writing by GlobalPlatform.
  - The laboratory must be free of any past fraudulent or criminal activity.
- 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. Also the laboratory should maintain all other insurance required by the applicable laws or regulations in the jurisdictions where laboratory's services are performed.

- Legal
  - The laboratory must be recognized as a legal entity and must be (or must be part of) an organization that is 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.
  - The laboratory must be able to sign and abide by all GlobalPlatform legal agreements for accredited testing laboratories, including **GlobalPlatform Security Laboratory Relationship Agreement**.
- Public Communications
  - The laboratory agrees to abide by GlobalPlatform's policy that testing performed at any GlobalPlatform Accredited Security Laboratory is acceptable for TEE approval, and must make no claims to the contrary in its marketing material.
  - The laboratory must not, under any circumstances, communicate nor disclose to any third party, including to the TEE Vendor or other entity submitting a product for testing, 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 conforms to the TEE Security Requirements.
- Independence
  - The laboratory must be able to demonstrate independence in evaluation methodology and from the party involved in the design or manufacturing of the product under evaluation.
  - The laboratory must not be owned by a product vendor involved in the creation of a TEE product without prior agreement from GlobalPlatform.
  - A laboratory must 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 of TEE related products.
  - The laboratory must not evaluate a product that it has been involved in, except that it may provide quality assurance testing (debug sessions) prior to the product vendor submitting the product for official GlobalPlatform TEE Security Evaluation.
  - The laboratory must receive communication and direction related to GlobalPlatform TEE Security Evaluation only from GlobalPlatform.
- Consistent Business Practices
  - It is mandatory that test results from a GlobalPlatform Accredited Security Laboratory are recognized by all other GlobalPlatform Accredited Security Laboratories, without any further investigation and without any discrimination regarding pricing for complementary testing.

4.3.3 Administrative Requirements

This section describes the administrative requirements that a laboratory must meet.

4.3.3.1 Quality Assurance

The laboratory must have a quality system based upon ISO requirements, providing documented procedures defining processes to ensure a high quality of testing and test reproducibility. These procedures must include, for example:

- Test methods and procedures
- Reporting of tests aimed at reproducibility and consistency
- Laboratory practices such as laboratory log books
- Procedures for maintaining accuracy and availability in equipment, including periodic calibration and justification of all measurement tools used for testing
- Procedures for test sample identification and secure storage
- Procedures for maintaining confidentiality of entrusted information

The laboratory must maintain an up-to-date library of technical reference material (books, papers, articles, etc.) on methods, standards, techniques, and equipment that are resident in the laboratory and that provide information required for laboratory test performance. The laboratory must also maintain up-to-date records of equipment maintenance.

The level of the above quality requirements and other requirements has been described in various international standards. A laboratory shall comply with [ISO 17025] and must also comply with the requirements stated elsewhere in this document.

4.3.3.2 Personnel

The laboratory must maintain a list of their qualified test personnel consisting of a description of their role in the organization, their qualifications, and their experience. The laboratory must have procedures to ensure a match between staff training and roles in the performance of GlobalPlatform activities.

Personnel Information

The laboratory must maintain a file in the personnel office for each employee. These files must be available to the GlobalPlatform Qualified Auditor during site visits and must clearly document the employment history including any background checks conducted on the employee.

The file must include, but is not limited to, the following (if legally permissible):

- Employee resume and job application
- Training programs, especially those involving any GlobalPlatform testing process or GlobalPlatform-qualified test tools
- Current photograph, updated at least every three years
- Verification of aliases (when applicable)
- Level of formal education
- Appropriate national identification number
- Signed document indicating that the employee has read and received a copy of the laboratory's policies and procedures

When employees are terminated, the laboratory must have designated staff members who execute and document the following:

- Recover the employee's photo ID badge or access card, access keys, or passes and immediately deactivate any access devices.
- Ensure that the employee surrenders all property and documentation involving GlobalPlatform testing and approval processes.
- Ensure that all computer (local area network [LAN]) access passwords are revoked or changed.
- Complete an employee termination checklist, which must include the above as a minimum.

4.3.4 Technical Requirements

This section describes the technical requirements for a laboratory conducting TEE Security Evaluation.

4.3.4.1 Technical Expertise

The following are examples of education or training for personnel performing the test and reviewing results:

- Computer Science
- Mathematics
- Cryptography
- Microelectronics

A GlobalPlatform Accredited Security Laboratory must have staff with an expert level of knowledge in the following areas:

- TEE specifications (training)
- Chipset architecture
- Trusted Computing
- And in at least one of the connected devices that execute the TEE: mobile, set-top boxes, payment terminals.

It is not necessary that each member of the laboratory's staff have knowledge and skills in each of these areas, but the laboratory staff as a whole must have at least one expert with the expected level of knowledge in each identified areas. Those experts must be part of the evaluation team. Any departure or organization modification that impacts the role of the TEE experts in the laboratory needs to be reported to the Global Platform Security Evaluation Secretariat.

Laboratory personnel must be skilled in using the laboratory equipment and applying the laboratory techniques.

4.3.4.2 Experience

The laboratory must have three (3) years of experience in security testing and its staff must have three (3) years of experience in testing: chip and/or chipset, microkernels and connected devices.

4.3.4.3 Equipment

The laboratory must have access to the necessary equipment to perform the evaluations such as described in [TEE EM].

The laboratory must have GlobalPlatform-qualified test tools with the latest TEE Test Suite.

4.3.5 Laboratory Security Requirements

This section describes the minimum security requirements that a laboratory must meet.

4.3.5.1 Physical Security

The laboratory must maintain and comply with a physical security policy that includes, at a minimum, the following requirements.

Physical Layout

The laboratory must have sufficient security measures to prevent unauthorized people from entering the building. If the laboratory is part of a shared building or complex, there must be sufficient security measures to prevent unauthorized people from entering the laboratory or offices.

Evaluation Areas

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.

Entry to the evaluation area must be restricted to authorized employees.

Storage

Within the laboratory there must be sufficient secure storage space to provide adequate protection for all on-going work. Additional secure storage must be provided for all materials retained by the laboratory after evaluation has been completed.

4.3.5.2 Logical Security

The laboratory must maintain and comply with a logical security policy that includes, at a minimum, the following requirements.

Classified Materials and Information

Test samples, documents, and specifications must be handled with particular care and kept within the company such that they are accessible only to persons appointed by the business management. These materials must be controlled and stored securely whether in electronic or paper format. Disclosure of GlobalPlatform or product vendor data and documents to third parties must be authorized in writing by an officer of the company that owns the data or documents to be released. Receipt of restricted information must be acknowledged by signature of the company's official representative.

Classified material must be stored in secure containers, where unauthorized access is prevented by appropriate measures (e.g. alarms, surveillance, and sufficient mechanical protection).

The laboratory must hold in strict confidence any classified information received from GlobalPlatform and product vendors. Classified documents must be stored according to their classification level. When a product vendor grants permission to the laboratory to release classified information concerning the product vendor's product to GlobalPlatform, this information may be released only to GlobalPlatform. The GlobalPlatform Security Evaluation Secretariat will release the information to appropriate working group members within GlobalPlatform.

Evaluation Reports

All evaluation reports must be stored securely. If reports are stored electronically, they must be in an industry-recognized protected form. All back-up processes must be appropriately managed by the laboratory according to industry standards for recovery purposes.

The laboratory must store samples and all reports and logs from the evaluations (whether paper or electronic) for a period of six (6) years following the expiration date of the certificate.

Note: *If the product is renewed by GlobalPlatform, the laboratory must store samples, test reports, and test logs for an additional six years after the expiration date of the new certificate.*

When issuing a paper report, the report must be issued in a tamper-evident package with a listed unique number.

When issuing an electronic report to GlobalPlatform, the report must, at a minimum, be password-protected using GlobalPlatform standard technique. Passwords must never be sent in the same email as the actual report. Passwords for GlobalPlatform may not be shared with third parties or Product Vendors.

Test Equipment Access

Non-test personnel must not be able to gain access to test software or test networks.

Test Equipment Hardware Maintenance

Any maintenance work on test equipment hardware and hardware systems must be authorized before work begins. The work must be performed under the control and authorization of the laboratory's staff, and there must be a documented procedure signing the equipment over to maintenance and signing the equipment back to production.

Test Equipment Software Maintenance

Test equipment software must be protected from unauthorized modification.

The update of the test software must be performed under continuous supervision of the laboratory's staff. If test tool equipment must be sent to the vendor or supplier to upgrade the tool software, there must be documented procedures and security controls for signing the test equipment over to the test equipment vendor or supplier and signing the equipment back to production.

Networks

All systems that are used to handle test data or constituent parts of test data must be, where possible, on a dedicated isolated network.

Any computers used to store secure information (evaluation reports, TEE Vendor data, etc.) must not be connected to an external network or to an internal network that allows unauthorized personnel access.

If the laboratory uses a non-dedicated network, then suitable controls must be in place to protect the integrity of the data within the laboratory. These controls include the use of firewalls and routers that offer sufficient security levels for the data being handled.

Networks linking the laboratory to third parties for the transfer of customer information must be separate and isolated from the test system, either physically or using network filters and adequate authentication.

Networks that link separate laboratory premises must use the network controls described above and all security sensitive data must be encrypted when using such networks.

The laboratory must have a secure method of transferring customer data to test samples and equipment that does not introduce security risks or vulnerabilities.

4.4 Audit Requirements

This section describes information that the laboratory is required to supply to the GlobalPlatform Qualified Auditor, and the level of detail required in the **Audit Reports**. The GlobalPlatform Qualified Auditor, in reviewing the documentation, may request additional information from the laboratory prior to or during the site visit and/or the demonstration of testing capabilities.

In preparation for the audit, the laboratory will provide written consent for disclosure of this information to GlobalPlatform and to the GlobalPlatform Qualified Auditor during the site visit.

The Audit Report that GlobalPlatform receives from the GlobalPlatform Qualified Auditor must have the level of detail specified in this section.

In order to prove conformance to the GlobalPlatform Accredited Security Laboratory requirements, the laboratory must do the following:

- Provide written evidence to the GlobalPlatform Qualified Auditor before the audit
- Complete a site visit
- Demonstrate testing capabilities
- Complete a **Corrective Action Plan**, if applicable

4.4.1 Written Evidence

4.4.1.1 Business Conformance

The laboratory provides the GlobalPlatform Qualified Auditor with evidence of conformance to the laboratory business requirements.

This evidence may be in the form of a written report describing:

- Services of the organization
- Structure of the organization, demonstrating the isolation between the laboratory and other areas of the organization (e.g. design area)
- Percentage of revenue received from each of the laboratory's top ten vendor customers relative to the total revenue of the laboratory

In addition, the laboratory must provide the GlobalPlatform Qualified Auditor with the following:

- Audited financial statements for the organization
- Official Annual Report as required by national or international law and/or regulation
- Certificate of ownership and/or tax identification number

4.4.1.2 Security Conformance

The laboratory provides to the GlobalPlatform Qualified Auditor evidence of physical and logical security conformance. This evidence must be in one of the following forms:

- Included within laboratory procedures and documentation, or
- A written report describing:
  - Laboratory security policy with particular focus on the physical and logical network security measures
  - Personnel background check security policies
  - Confidential data protection practices

4.4.2 Administrative Conformance

The laboratory provides to the GlobalPlatform Qualified Auditor evidence of administrative conformance. This evidence may be in the form of a written report describing:

- Formal accreditations
- Experience relevant to the desired laboratory role
- Description of the laboratory's quality assurance system

The quality assurance system must comply with the requirements of the GlobalPlatform process and follow the [ISO 17025]. As such, the description must contain, for instance:

- Overview of the laboratory personnel and the qualifications of laboratory personnel involved in the performance of any testing or administrative duties connected with TEE security evaluation.
- Overview of the laboratory equipment and techniques
- Description of the laboratory security policy with particular focus on the procedures for identification and recording of test samples
- Overview of laboratory asset management system for documentation and equipment

4.4.3 Site Visit

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

- Verify that laboratory documentation and actual laboratory implementation are in agreement.
- Observe the physical environment of the organization and the physical security measures taken.
- Verify that the laboratory's personnel information is on file (if it is legally permissible for the Qualified Auditor to examine this information).
- Verify the laboratory's technical expertise.
- Verify the laboratory's quality assurance procedures and [ISO 17025] certificate.
    - The laboratory provides a copy of the Audit Report corresponding to the [ISO 17025] certificate to the GlobalPlatform Qualified Auditor. Otherwise, the Auditor requests a copy from the issuing organization.
    - The GlobalPlatform Qualified Auditor reviews the Audit Report to use as evidence of compliance in the Audit Report for GlobalPlatform and audits the laboratory for the GlobalPlatform requirements that are not covered by the [ISO 17025] certificate.

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

4.4.4 Demonstration of Testing Capabilities

GlobalPlatform may require a demonstration of the laboratory's actual testing capabilities. This will be done through witnessing the laboratory's testing of a product or through pilot testing.

Pilot testing is defined as the laboratory's performing testing on a previously certified TEE product or on a simulation product and providing a test report to the GlobalPlatform Qualified Auditor to review. The choice of subject for this pilot testing is at the discretion of GlobalPlatform and GlobalPlatform reserves the right to witness a part of this evaluation.

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

4.4.5 Corrective Action Plan

An Audit Report may indicate that the laboratory does not meet all necessary requirements, but has demonstrated sufficient capabilities that with specific corrective actions, it would do so. If so:

- The laboratory will define a **Corrective Action Plan** with deliverables and due dates to meet all GlobalPlatform requirements.
- The GlobalPlatform Qualified Auditor will review and validate the **Corrective Action Plan**, then provide a copy of the validated **Corrective Action Plan** in its **Audit Report** to GlobalPlatform.

GlobalPlatform, when reviewing the **Audit Report**, will review the **Corrective Action Plan** and, if the plan is acceptable, may grant accreditation on a provisional basis and set a date when an **Interim Proficiency Audit** will be required.

The **Interim Proficiency Audit** will ensure that the laboratory has met all of the requirements identified in the **Corrective Action Plan**.

4.5 Accreditation Termination

At any time, a GlobalPlatform Accredited Security Laboratory's **Relationship Agreement** with GlobalPlatform may be modified or terminated:

- A laboratory may decide to terminate its accreditation.
- GlobalPlatform may decide to suspend or revoke a laboratory's accreditation.

4.5.1 Termination by the Laboratory

At any time, a laboratory may request termination of its GlobalPlatform **Security Laboratory Relationship Agreement**.

Upon receipt of such request, GlobalPlatform will confirm termination of the laboratory's **Security Laboratory Relationship Agreement** and accreditation and remove the laboratory's name from the list of accredited laboratories on the GlobalPlatform website.

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

4.5.2 Suspension or Revocation by GlobalPlatform

Suspension

At any time, at GlobalPlatform's own discretion, GlobalPlatform may suspend a laboratory's accreditation:

- Based on the results of an **Audit Report**
- Due to a laboratory's nonconformance
- Due to GlobalPlatform membership fees in arrears
- If a laboratory fails to complete an **Incremental Audit** or **Interim Proficiency Audit** to the satisfaction of GlobalPlatform by the required date

If the accreditation of a laboratory is suspended:

- The name of the laboratory will be removed from the list of accredited laboratories
- GlobalPlatform will set the requirements and the date by which another **Interim Proficiency Audit** must be completed

Revocation

At any time and at GlobalPlatform's own discretion, GlobalPlatform may revoke a laboratory's accreditation:

- Based upon the results of an **Audit Report**
- Due to a laboratory's nonconformance
- Due to a laboratory's failure to maintain GlobalPlatform membership in good standing
- If a laboratory has not performed testing on TEE products within the last two years
- If a laboratory fails to renew its accreditation before it expires

Revocation of accreditation automatically terminates the **GlobalPlatform Security Laboratory Relationship Agreement** with the laboratory. GlobalPlatform will also remove the laboratory's name from the list of accredited laboratories on the GlobalPlatform website.

Upon GlobalPlatform's revocation of a laboratory's accreditation, the laboratory must make available to GlobalPlatform all test reports, test logs, and samples for products already evaluated by GlobalPlatform or currently in evaluation for GlobalPlatform Certification.

The laboratory must also promptly return to GlobalPlatform all GlobalPlatform property and all confidential information. Alternatively, if so directed by GlobalPlatform, the laboratory must destroy all confidential information, and all copies thereof, in the laboratory's possession or control, and must provide a certificate signed by an officer of the laboratory that certifies such destruction in detail acceptable to GlobalPlatform.

5 Security Evaluation and Certification Process

5.1 Certifiable Products

Certifiable TEE products can be hosted in a prototype or in a device.

At GlobalPlatform's discretion, it can be a product family. Acceptable variation within a family is up to GlobalPlatform's decision.

Certifiable TEE products shall fulfill all mandatory requirements especially for functional testing that are detailed in [TEE EM]. In addition, [TEE EM] specifies the necessary conditions that enables a no more than three (3) months evaluation.

5.2 Types of Evaluations

The GlobalPlatform Certificate may be one of three types:

- Full Evaluation: A full evaluation 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 [TEE PP] and the selected PP-modules.
- Delta Evaluation: A delta evaluation applies to a TOE that is an updated version of a certified TOE (original TOE). In the case of a product update, the vendor must provide an **Impact Analysis Report** describing all the product changes to GlobalPlatform Security Evaluation Secretariat. GlobalPlatform Security Evaluation Secretariat whether delta evaluation type is adequate.
- Fast Track Evaluation: The fast track evaluation can be used for changes to the original TOE with valid certificate that do not impact its security. GlobalPlatform Security Evaluation Secretariat will decide whether fast track evaluation type is adequate. Indeed, any security change has to be evaluated in full or delta evaluation.

The product vendor shall refer to the TEE Evaluation Methodology [TEE EM] for more details on evaluation type.

5.3 Security Evaluation Roles

The following sections describe the various roles of the actors during the GlobalPlatform TEE Certification Process.

5.3.1 GlobalPlatform Security Evaluation Secretariat

For all evaluations:

- Maintains TEE Security Requirements through the TEE Security Working Groups
- Security Monitoring (see section 5.5.5)
- Provides Forms and Agreements

For each evaluation:

- Provides the **Security Evaluation Agreement**
- Validates the **Product Evaluation Request Form**
- Validates the **Security Evaluation Reports (DTER and TER)**
- Establishes the **Risk Analysis Report** with the TEE Vendor (if applicable)
- Issues (Restricted) Certificates for successfully evaluated Products
- Publish certificates under the TEE Certification Scheme page of www.globalplatform.org unless otherwise instructed by the TEE Vendor.

5.3.2 Product Vendor

For each evaluation:

- Fills the appropriate **Product Evaluation Request Form**
- Selects the Evaluation type (Full, Delta, Fast Track)
- Signs the **Security Evaluation Agreement**
- Selects and contracts with the GlobalPlatform Accredited Security Laboratory
- Provides GlobalPlatform with **Impact Analysis Report** when applicable
- Provides the laboratory with the necessary inputs (Security Target, documentation, sample)

5.3.3 GlobalPlatform Accredited Security Laboratory

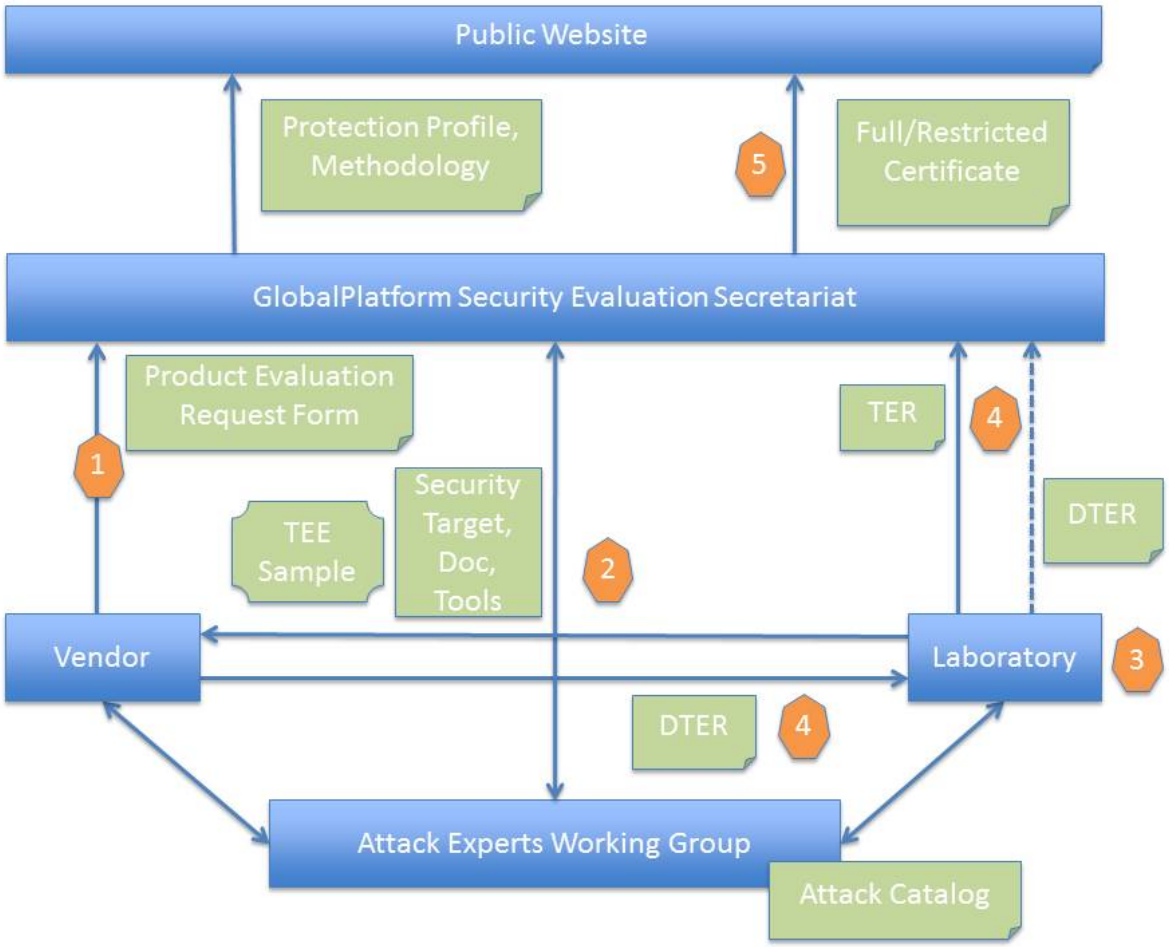
For each evaluation:

- Challenges the Impact/security analysis
- Validates the Security Target created from the template [TEE ST]
- Tests the Product
- Writes the **Security Evaluation Reports (DTER and TER)**

5.4 TEE Certification Process Flow

The remaining sections of this chapter describe the individual actions within the GlobalPlatform TEE Certification Process, as shown in Figure 5-1.

Figure 5-1: GlobalPlatform TEE Certification Process Flow



5.4.1 Product Evaluation Request

The product vendor shall request an **Product Evaluation Request Form** from GlobalPlatform at teecertification@globalplatform.org, then shall submit the completed **Product Evaluation Request Form** defining details of the product intended for evaluation, related administrative information, and technical information including: the Security Target created based on the template [TEE ST] and the list of evidences of any security independent evaluations already carried out on the product. This will enable the GlobalPlatform Security Evaluation Secretariat staff to approve evaluation start and confirm the type of evaluation: Full, Delta, or Fast Track.

GlobalPlatform and the product vendor sign a **GlobalPlatform Security Evaluation Agreement** covering the GlobalPlatform TEE Certification Process.

5.4.2 Evaluation Start

The product vendor shall contract the GlobalPlatform Accredited Security Laboratory on the basis of the approved **Product Evaluation Request Form**. The vendor provides the laboratory with all the mandatory information, samples, and tools described in [TEE EM].

5.4.3 Product Assessment

The evaluation of the TEE includes a threat and vulnerability assessment of identified security assets. The vulnerability analysis is described in [TEE EM]. It includes a set of common automated and non-automated tests. The laboratories perform the required evaluation and provide evaluation reports documenting the results.

5.4.4 Evaluation Reports

After evaluation, the GlobalPlatform Accredited Security Laboratory issues a **Detailed TEE Evaluation Report (DTER)** and a **TEE Evaluation Report (TER)**. The content is described in [TEE EM].

The conclusions of the Evaluation Reports should:

- be based on guidance provided in [TEE PP], [TEE EM], and [TEE AP] (the TEE Security Requirements),
- include sufficient reporting of penetration testing to prove that the tests were completed as appropriate in order to reach the conclusions on the assurance level claimed EAL2+ (especially AVA_TEE). (This allows product vendors to re-use the results of their Common Criteria evaluations if they so choose.)

The TER is transmitted to the vendor and GlobalPlatform. Additionally, the laboratory issues a DTER to GlobalPlatform, if requested by the GlobalPlatform Security Evaluation Secretariat.

5.4.5 Certification

Evaluation Reports Review

The GlobalPlatform Security Evaluation Secretariat reviews the TER and may request details of evaluation information, or require a DTER report from the laboratories and ask further evaluation to be performed.

The GlobalPlatform Security Evaluation Secretariat will use the current Attack Catalog [TEE AP] to base its final judgment.

If the GlobalPlatform Security Evaluation Secretariat considers that the evaluation provides sufficient assurance that a product complies with the GlobalPlatform TEE Security Requirements, the GlobalPlatform Security Evaluation Secretariat prepares a **GlobalPlatform Certification Report**.

Risk Analysis Report (when applicable)

Based on the evaluation results, and the report generated as a result of the previous process step (**GlobalPlatform Certification Report**), the product vendor and the GlobalPlatform Security Evaluation Secretariat together perform an assessment of the risks resulting from the vulnerabilities discovered.

The product vendor may decide to remedy the vulnerabilities discovered and re-start the GlobalPlatform TEE Certification Process.

If residual vulnerabilities are discovered that the GlobalPlatform Security Evaluation Secretariat considers significant enough to result in the issue of an **GlobalPlatform Restricted Security Evaluation Certificate**, and the product vendor decides not to remedy these vulnerabilities, the product vendor and the GlobalPlatform Security Evaluation Secretariat jointly prepare a **Risk Analysis Report** containing information for TEE Users intending to use that vendor's product.

The GlobalPlatform Security Evaluation Secretariat will attempt to understand the product vendor's wishes with respect to the content of the **Risk Analysis Report**. However, GlobalPlatform reserves its final authority over the content of this **Risk Analysis Report** to provide TEE Users with reliable information for a valid risk assessment of their TEE projects.

GlobalPlatform Security Evaluation Certificate Issuance

If the GlobalPlatform Security Evaluation Secretariat concludes that sufficient assurance has been demonstrated in the **GlobalPlatform Certification Report**, GlobalPlatform will issue the product vendor with a **GlobalPlatform Security Evaluation Certificate** for that product.

If the GlobalPlatform Security Evaluation Secretariat concludes that vulnerabilities discovered during the evaluation process are being satisfactorily addressed by the Product Vendor and are sufficiently explained by the **Risk Analysis Report**, GlobalPlatform may issue the product vendor with a GlobalPlatform **Restricted Security Evaluation Certificate** for that product. Each certificate will contain a TEE Security Certificate Number (TEESCN), a unique four-digit reference number identifying the TEE that has been certified, and its related devices.

5.5 Certificate Management

TEE Security Evaluation Certificates issued by GlobalPlatform confirm that the product vendor's product(s) identified on the Certificate have undergone the appropriate security evaluation, and that a risk analysis on any significant residual vulnerability has been performed (where applicable).

5.5.1 Full/Restricted Certificate

A TEE Security Evaluation Certificate may be issued in one of two variants (Full/Restricted), depending on whether any significant residual vulnerability was discovered during the evaluation process. If any residual vulnerability discovered during the evaluation process is considered by the GlobalPlatform Security Evaluation Secretariat to be below the level that GlobalPlatform regards as significant, then GlobalPlatform will issue a **GlobalPlatform Security Evaluation Certificate** for that product.

If significant residual vulnerabilities are discovered during the evaluation process but are considered a manageable risk by the GlobalPlatform Security Evaluation Secretariat, are sufficiently explained in the **Risk Analysis Report**, and are being satisfactorily addressed by the product vendor, GlobalPlatform will issue a **GlobalPlatform Restricted Security Evaluation Certificate** for that product.

GlobalPlatform is entitled to publish non-security related details of restricted certificates. Consequently, the product vendor will be required to inform the TEE Users (or other product vendors to whom that product vendor intends to sell the product covered by an GlobalPlatform **Restricted Security Evaluation Certificate**) of the product vulnerabilities so they may understand the risk in using the restricted product. This is necessary so that the product vendor's customers can accommodate the remaining risks within their own risk assessments, and introduce appropriate countermeasures against these remaining risks into their own systems.

The Certificates and related information can remain confidential if the vendor is requesting it.

5.5.2 Certificate Content

The Certificate includes:

- an identification of the product
- a list of actors who participated in the certification
- a list of the TEE Security Requirements documents and versions used
- the issuance date and the validity date

5.5.3 Validity

The Certificate is valid for three (3) years.

5.5.4 In Case of Delta or Fast Track Evaluation

A Delta or Fast Track Evaluation issues a Derived Certificate. The Derived Certificate validity date is identical to the validity date of the original Certificate. There is no Certificate renewal process defined.

5.5.5 Security Monitoring

The GlobalPlatform Security Evaluation Secretariat continuously monitors threats and security developments within the TEE market. It monitors new threats and attacks, with GlobalPlatform TEE Security Working Group and subgroups.

Where it considers this necessary (and where it is able to do so given confidentiality restrictions) the GlobalPlatform Security Evaluation Secretariat may inform product vendors about newly discovered vulnerabilities of their certified products, thus enabling and supporting the product vendor to minimize consequent risks, and to support their customers' risk management. This may also include the withdrawal of a GlobalPlatform **Security Evaluation Certificate** or a GlobalPlatform **Restricted Security Evaluation Certificate**.

- The GlobalPlatform Security Evaluation Secretariat shall inform vendors in advance when a new version of the Attack Catalog [TEE AP] will be applicable.
- Appearance of a new attack is managed by the TEE Attack Experts Working Group and GlobalPlatform Security Evaluation Secretariat.

5.5.6 Publication on GlobalPlatform Website

In agreement with the product vendor, GlobalPlatform shall publish the list of certified products together with the appropriate certificate under the TEE Certification Scheme page of www.globalplatform.org.

It is the responsibility of the product vendor and TEE Users to verify the version of [TEE AP] listed in the certificate.