GLOBALPLATFORM™

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform Technology

TEE Security Target Template

Version 1.0.0

Final Release

November 2015

Document Reference: GPD_TEN_045

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 template of TEE Security Target, based on the TEE Protection Profile, required to apply for GlobalPlatform TEE security certification [TEE CP, TEE EM].

The Security Target shall contain all the information required in sections 1 to 6.

The functional description required in Section 7 is mandatory in the case of a three-months full evaluation.

1.1 Audience

This template is intended to TEE developers/vendors and TEE laboratories. Section 1.1 is not mandatory in the Security Target. The ST writer may introduce its own information in this section.

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.

Section 1.2 is not mandatory in the Security Target. The ST writer may introduce its own information in this section.

1.3 References

Section 1.3 is mandatory in the Security Target. The Security Target writer shall give the actual applicable “normative references”.

The Table “Informative references” shall include the references of the non-GlobalPlatform APIs implemented by the TOE and also of the identification of pre-loaded TAs, if applicable.

Table 1-1: Normative References

Standard / Specification	Description	Ref
GP_PRO_023	GlobalPlatform Device Technology TEE Certification Process (last applicable version)	[TEE CP]
GPD_GUI_044	GlobalPlatform Device Technology TEE Evaluation Methodology (last applicable version)	[TEE EM]
GPD_SPE_007	GlobalPlatform Device Technology TEE Client API Specification v1.0	[TEE CLIENT 1.0]

Standard / Specification	Description	Ref
GPD_EPR_028	GlobalPlatform Device Technology TEE Client API Specification v1.0 Errata and Precisions v2.0	[TEE CLIENT E 2.0]
GPD_SPE_010	GlobalPlatform Device Technology TEE Internal Core API Specification v1.0	[TEE CORE 1.0]
GPD_EPR_017	GlobalPlatform Device Technology TEE Internal Core API Specification v1.0 Errata and Precisions v1.0	[TEE CORE E 1.0]
	GlobalPlatform Device Technology TEE Internal Core API Specification v1.0 Errata and Precisions v3.0	[TEE CORE E 3.0]
GPD_SPE_024	GlobalPlatform Device Technology TEE Secure Element API Specification v1.0	[TEE SE 1.0]
GPD_EPR_030	GlobalPlatform Device Technology TEE Secure Element API Specification v1.0 Errata and Precisions v1.0	[TEE SE E 1.0]
GPD_SPE_020	GlobalPlatform Device Technology Trusted User Interface API Specification v1.0	[TEE TUI 1.0]
GPD_SPE_025	GlobalPlatform Device Technology TEE TA Debug Specification v1.0	[TEE TA DEBUG 1.0]
GPD_SPE_013	GlobalPlatform Device Technology Secure Element Access Control v1.0	[TEE SEAC 1.0]
	GlobalPlatform Device Technology Secure Element Access Control v1.1	[TEE SEAC 1.1]
	TEE Initial Configuration Test Suite v1.1.0.1	[TEE ICTS 1.1.0.1]
GPD_SPE_021	TEE Protection Profile PP-configuration composed of the base Protection Profile only v1.2	[TEE PP 1.2]
GPD_SPE_021 +Time	TEE PP-configuration composed of the base Protection Profile and the TEE Time and Rollback PP-module v1.2	[TEE PP T 1.2]
GPD_SPE_021 +Debug	TEE PP-configuration composed of the base Protection Profile and the TEE Debug PP-module v1.2	[TEE PP D 1.2]
GPD_SPE_021 +Time&Debug	TEE PP-configuration composed of the base Protection Profile and the TEE Time and Rollback and TEE Debug PP-modules v1.2	[TEE PP TD 1.2]
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]

Table 1-2: Informative References

Reference	Standard / Specification	Ref
	Any other API implemented by the TOE	
	Specification of preloaded TAs	

1.4 Terminology and Definitions

Section 1.4 is not mandatory in the Security Target.

1.4.1 Key Words

The key words “MUST”, “MUST NOT”, “SHALL”, “SHALL NOT”, “REQUIRED”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document indicate normative statements and are to be interpreted as described in [RFC 2119].

The ST writer may define key words in this section.

1.4.2 Other Terminology

The ST writer may define all terminology in this section.

Selected terms used in this document are included in Table 1-3. Additional terms are defined in the references.

Table 1-3: Terminology and Definitions

Term	Definition

1.5 Abbreviations and Notations

The ST writer may explain all abbreviations and notations in this section.

Selected abbreviations and notations used in this document are included in

Table 1-4. Additional abbreviations and notations are defined in the references.

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning

Abbreviation / Notation	Meaning

1.6 Revision History

While the document is being developed, record at least the versions that are delivered to third parties, including GlobalPlatform Security Evaluation Secretariat and laboratory. You may include entries describing each draft, if desired.

When the document is published or the final version released, you may wish to remove all entries except those for the published versions

Table 1-5: Revision History

Date [day month year]	Version	Description
[day month year]	[0.*n.n.n*]	
[day month year]	[0.*n.n.n*]	
[day month year]	[0.*n.n.n*]	
[day month year]	1.0	

2 Identification

2.1 Security Target Identification

The writer of the Security Target shall fill-in the following identification table.

Security Target Identification	
Document title	
Document reference	
Document version	
Document publication date	
Document status	*Draft – Final* *Confidential – Restricted - Public* *or any other classification used in your company*
Document author	*Name and company*

2.2 TOE Identification

2.2.1 TOE Type

The writer of the Security Target shall fill-in the following characterization table.

TOE characterization	
TOE Type	*System-on-Chip, Device or both*
Multiple TOEs	*Yes/No* *(this information has to match the identification tables below)*

2.2.2 TOE References

In the following table, “reference” stands for a unique identifier including the version number and release date if applicable. The references are those used in the developer/manufacturer configuration management system(s).

The writer of the Security Target shall fill-in the applicable identification tables.

The following identification table is applicable to Device type of TOE. The ST writer shall provide as many tables as necessary to cover the Devices within the scope of evaluation.

Device name	Device reference	Main developer	SoC reference
List of commercial names	*List of references per name*	*Main developer per reference*	*List of applicable SoC references per device reference*

The following identification table is applicable to all types of TOE. The ST writer shall provide as many tables as necessary to cover the SoCs within the scope of evaluation.

SoC Identification	
SoC reference(s)	*Unique identifier(s)*
Commercial name(s)	*Name(s) or N/A*
Main developer	*Name*
Hardware reference	*Unique identifier*
ROM code reference	*Unique identifier*
Boot code reference	*Unique identifier*
TEE binary reference	*Unique identifier*
Comments	*Free text. For instance, explanation if many SoC references apply to the same HW/SW combination, which may happen for families of TOEs.*

2.3 Non-TOE Components Identification

The writer of the Security Target shall provide the references of the non-TOE components that are required for the operation of the TEE or that have some interface with the TOE, for instance, Rich OS, NFC Controller, Fingerprint sensors, etc.

Non-TOE components identification			
Name	**Reference**	**Main developer**	**SoC/Device reference**
List of commercial names	*List of references per name*	*Main developer per reference*	*List of SoC and/or Device references to which these non-TOE components are applicable*

The writer of the Security Target shall also indicate the references of the Trusted Applications that are pre-loaded in the TOE.

Pre-loaded TA identification	
TA identifier	*Unique identifier*
Commercial name(s)	*Name(s) or N/A*
Main developer	*Name*
TA binary reference	*Unique identifier*
TEE guidance version(s)	*Reference(s) of the guidance that has been used*
Comments	*Purpose of the TA, if there is no guidance referenced why, etc.*

2.4 Security Guidance Identification

The writer of the Security Target shall fill-in the following security guidance identification table. One table per applicable guidance document:

- Guidance for SoC integrators: mandatory for SoC type of TOE
- Guidance for TA developers: mandatory for SoC and Device type of TOE.
- Guidance for TEE final users: mandatory for Device type of TOE

Guidance for SoC integrators	
Document title	
Document reference	
Document version	
Document publication date	
Document status	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*
Comments	*Free text.*

Guidance for TA developers	
Document title	
Document reference	

Guidance for TA developers	
Document version	
Document publication date	
Document status	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*
Comments	*Free text*

Guidance for TEE final users	
Document title	
Document reference	
Document version	
Document publication date	
Document status	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*
Comments	*This guidance may not be a document but a commercial notice.* *Explain if there is no action or behavior expected from TEE final user (the fields above are empty)*

2.5 Developers and Manufacturers Identification

The writer of the Security Target shall fill-in the following developer & manufacturer identification table.

Developer/ Manufacturer Company Name	Legal Address	Contact	TOE-related sites	Site audits/date
			Sites involved in the development / manufacturing of the TOE	*For each site, list of audits performed the last three years (referential if applicable, for instance ISO 9001, auditor, date)* *And indication if the audit covered or not the TEE-related activities and organization*

3 Compliance Claims

3.1 GlobalPlatform API Functional Compliance

The writer of the Security Target shall fill-in the following API identification table indicating the type of compliance with GlobalPlatform specifications (CF, DF, DP or NI) for each TEE API:

- "Certified Full functional compliance" (CF): means that the TOE fully implements an approved version of the API and that the TOE has successfully passed GlobalPlatform functional compliance testing for this API. The Vendor shall provide the GlobalPlatform Letter of Qualification (LOQ).
- "Declared Full functional compliance" (DF): means that the TOE fully implements an approved version of the API but the compliance has not been qualified by GlobalPlatform.
- "Declared Partial functional compliance" (DP): means that the TOE partially implements an approved version of the API. The Vendor shall identify the compliant/non-compliant parts of the API.
- "Not Implemented" (NI): the TOE does not implement the API.

Reference	GlobalPlatform Device Technology	V.	Compliance type
GPD_SPE_007	TEE Client API Specification	1.0	
GPD_EPR_028	TEE Client API Specification v1.0 Errata and Precisions	2.0	
GPD_SPE_010	TEE Internal Core API Specification	1.0	
GPD_EPR_017	TEE Internal Core API Specification v1.0 Errata and Precisions	1.0	
	TEE Internal Core API Specification v1.0 Errata and Precisions	3.0	
GPD_SPE_024	TEE Secure Element API Specification	1.0	
GPD_EPR_030	TEE Secure Element API Specification v1.0 Errata and Precisions	1.0	
GPD_SPE_020	Trusted User Interface API Specification	1.0	
GPD_SPE_025	TEE TA Debug Specification	1.0	
GPD_SPE_013	Secure Element Access Control	1.0	
	Secure Element Access Control	1.1	
	Other GlobalPlatform specifications or versions (e.g. available to members only)		

The writer of the Security Target shall fill-in the following API identification table indicating the kind of compliance with GlobalPlatform TEE specifications:

Reference	GlobalPlatform Device Technology	V.	LOQ issuance date
	TEE Initial Configuration Test Suite	1.1.0.1	*Date or N/A*

Reference	GlobalPlatform Device Technology	V.	LOQ issuance date
	Other GlobalPlatform *test suites (e.g. available to members only)*		

3.2 Proprietary API

The writer of the Security Target shall fill-in the following table with the identification of the non-GlobalPlatform API implemented by the TOE:

Reference	Standard / Specification	V.	SFR-related
reference	*Any other API implemented by the TOE*	*Version number*	*Yes/No*

3.3 GlobalPlatform Protection Profile Compliance

The writer of the Security Target shall fill-in the following TEE PP identification table indicating the modules that are claimed together with the base-PP: Time&Rollback Module, Debug Module or both.

The requirements of the base-PP are mandatory.

Reference	GlobalPlatform Device Technology	V.	Compliance
GPD_SPE_021	TEE Protection Profile (PP-configuration composed of the base Protection Profile only)	1.2	Yes
GPD_SPE_021+Time	TEE PP-configuration composed of the base Protection Profile and the TEE Time and Rollback PP-module	1.2	*Yes/No*
GPD_SPE_021+Debug	TEE PP-configuration composed of the base Protection Profile and the TEE Debug PP-module	1.2	*Yes/No*
GPD_SPE_021+Time&Debug	TEE PP-configuration composed of the base Protection Profile and the TEE Time and Rollback and TEE Debug PP-modules)	1.2	*Yes/No*

4 TOE Description

4.1 Expected Usage

This section shall contain a description of the expected usage of the TOE.

4.2 Overview

This section shall contain a description of the TOE hardware and software boundaries and components, i.e. the architecture and the physical and logical interfaces of the TOE, including the GlobalPlatform and proprietary APIs available to the TA's, the interface with the REE and the hardware interfaces to the TEE internals.

The overview shall also include a description of the TOE operation modes including debug modes (disabled or enabled).

4.3 Life Cycle

The ST writer shall describe the TOE life cycle. The following generic description provided in the PP can be used as guidance:

"Security Targets shall describe the actual TOE life cycle, identify the actors and development/manufacturing sites involved; they shall identify the actual integration points of the components (Trusted OS, root of trust, TAs) into the device, as well as the actual delivery point of the TOE, and precise the process for setting the root of trust of the TEE storage services and the phase in which it occurs.

Security targets shall also identify the TOE and the components that are delivered with the TOE if any, e.g. the standard OS, pre-installed Trusted Applications or Client Applications. If the TOE provides TA management functionality (i.e. installation of TAs in phase 6 or in general after the delivery point), which is not in the scope of this Protection Profile, it must be described in the ST as well."

5 Assumptions

The writer shall include in the ST all the assumptions on the TOE operational environment defined in the TEE PP and applicable modules. The ST writer can complete these statements with “application notes” to reflect the specificities of the TOE or its operational environment.

The ST writer shall not remove any applicable assumption.

The ST writer shall not add any assumption.

The ST writer shall not modify the non-red text.

The Security Target shall contain the following two assumptions

A.PROTECTION_AFTER_DELIVERY

It is assumed that the TOE is protected by the environment after delivery and before entering the final usage phase. It is assumed that the persons manipulating the TOE in the operational environment apply the TEE guidelines (e.g. user and administrator guidance, installation documentation, personalization guide). It is also assumed that the persons responsible for the application of the procedures contained in the guides, and the persons involved in delivery and protection of the product have the required skills and are aware of the security issues.

Application Note:

The certificate is valid only when the guidelines are applied. For instance, for installation, pre-personalization or personalization guides, only the described set-up configurations or personalization profiles are covered by the certificate.

The security target shall reference the applicable TEE guidelines, in particular the operational guidance that fulfills AGD_OPE.1 requirements.

A.TA_DEVELOPMENT

TA developers are assumed to comply with the TA development guidelines set by the TEE provider. In particular, TA developers are assumed to consider the following principles during the development of the Trusted Applications:

- CA identifiers are generated and managed by the REE, outside the scope of the TEE. A TA must not assume that CA identifiers are genuine
- TAs must not disclose any sensitive data to the REE through any CA (interaction with the CA may require authentication means)
- Data written to memory that are not under the TA instance's exclusive control may have changed at next read
- Reading twice from the same location in memory that is not under the TA instance's exclusive control can return different values.

The Security Target shall also contain the following assumption if it does not claim compliance claim with the Time&Rollback PP-Module.

A.ROLLBACK

It is assumed that TA developers do not rely on protection of TEE persistent data, TA data and keys and TA code against full rollback.

6 Security Functional Requirements

The writer shall include in the ST all the Security Functional Requirements (SFR) defined in the TEE PP and applicable modules and instantiate those that are (partially) open. The elements that require instantiation correspond to the following two operations:

- [selection: … list of selectable items …]
- [assignment: … list of authorized assignments…]

In the examples below, the operations are written in bold red police. The ST writer shall use red or any other color or police of their choice to highlight the TOE-specific instantiations.

The ST writer can complete these statements with “application notes” to explain or clarify the meaning of the SFR in the context of the TOE.

The following sections shall contain the SFRs defined in the TEE PP:

- Section 4.1 is mandatory.
- Section 4.2 is mandatory whenever the Time & Rollback PP-Module is claimed (cf. Section 3.3)
- Section 4.3 is mandatory whenever the Debug PP-Module is claimed (cf. Section 3.3)

The ST writer shall not remove any SFR from the TEE PP.

The ST writer shall not modify the non-red text of the SFRs.

6.1 TEE Base-PP

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **CA_identity, TA_identity, TA_properties, [assignment: list of security attributes]**.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

To be completed with the SFRs from TEE PP v1.2 (base-PP)

6.2 Time and Rollback PP-module

FDP_SDI.2/Rollback Stored data integrity monitoring and action

FDP_SDI.2.1/Rollback The TSF shall monitor TEE rollback detection data, TEE runtime data, TEE persistent data, TA data and keys and TA code stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **[assignment: attributes of TEE rollback detection data, TEE runtime data, TEE persistent data, TA data and keys and TA code]**.

FDP_SDI.2.2/Rollback

- Upon detection of integrity errors in TEE rollback detection data, TEE runtime data or TEE persistent data, the TSF shall **behave in a manner that does not depend on the compromised data**
- Upon detection of TA code integrity errors, the TSF shall **abort the execution of the TA instance**
- Upon detection of TA data or TA keys integrity errors, the TSF shall
  - **Not provide any compromised data,**
  - **Behave in a manner that does not depend on the compromised data**
  - **[assignment: other actions to be taken]**.

FPT_FLS.1/Rollback Failure with preservation of secure state

FPT_FLS.1.1/Rollback The TSF shall preserve a secure state when the following types of failures occur:

- **TA code and data integrity failure**
- **TEE persistent data integrity failure**.

To be completed with the SFRs from TEE PP v1.2 (Time&Rollback PP-Module)

6.3 Debug PP-module

FDP_ACC.1/Debug Subset access control

FDP_ACC.1.1/Debug The TSF shall enforce the **Debug access control SFP** on

- **Subjects: S.DEBUG**
- **Objects: all objects**
- **Operations: OP.ACTIVATE, OP.DEBUG**.

FDP_ACF.1/Debug Security attribute based access control

FDP_ACF.1.1/Debug The TSF shall enforce the **Debug access control SFP** to objects based on the following:

- **S.DEBUG.enabled, S.DEBUG.authenticated**

- **[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]**.

FDP_ACF.1.2/Debug The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **OP.AUTHENTICATE is allowed if the following conditions hold:**
  - **The operation is performed by S.DEBUG**
  - **The debug interface is enabled (S.DEBUG.enabled = True)**
- **OP.DEBUG on all objects is allowed if the following conditions hold:**
  - **The operation is performed by S.DEBUG**
  - **The debug interface is enabled (S.DEBUG.enabled = True)**
  - **The TEE Debug Administrator is authenticated (S.DEBUG.authenticated = True)**
- **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

FDP_ACF.1.3/Debug The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/Debug The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

To be completed with the SFRs from TEE PP v1.2 (Debug PP-Module).

7 Functional Description

This section is mandatory for a three-months full evaluation. It is optional otherwise.

The ST writer shall provide a functional description that explains how the TOE fulfills the SFRs, in particular the role of the hardware and software security mechanisms. References to external documentation are accepted.