GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
TEE Security Target Template
Version 1.1.0

Public release

May 20211

Document Reference: GPD_TEN_045

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
Recipients of this document are invited to submit, with their comments, notification of any relevant patents or other intellectual property rights (collectively, "IPR") of which they may be aware which might be necessarily infringed by the implementation of the specification or other work product set forth in this document, and to provide supporting documentation. The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. This documentation is currently in draft form and is being reviewed and enhanced by the Committees and Working Groups of GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

This document is provided as a member benefit to GlobalPlatform members only.
Please help us maintain the value of your membership and encourage recruitment by observing this restriction.

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Contents

Tables

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

1 Introduction

This document defines the template for the TEE Security Target (ST), based on the TEE Protection Profile (TEE PP), required to apply for a GlobalPlatform TEE security certification [TEE CP].

The ST shall contain all the information required in Sections 1 to 8.

The laboratory may require the functional description in Section 9. This information is mandatory for a three-months full evaluation.

1.1 Audience

This template is intended for TEE developers/vendors and TEE laboratories. Section 1.1 is not mandatory in the ST.

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 ST.

1.3 References

Section 1.3 is mandatory in the Security Target. Table 1-1 and Table 1-2 contain the references used in the present and other documents that are often referenced in TEE STs.

The ST author shall provide the actual applicable references, including version numbers.

The ST author shall provide the references of the proprietary APIs implemented by the TOE and the identification of pre-installed TAs, if applicable.

Table 1-1: GlobalPlatform References

Standard / Specification	Description	Ref
GPD_SPE_021	GlobalPlatform Technology TEE Protection Profile v1.3	[TEE PP]
GPT_SPE_141	GlobalPlatform Technology TEE PP-Module Time and Rollback v1.3	[PPM-TR]
GPT_SPE_140	GlobalPlatform Technology TEE PP-Module Debug v1.3	[PPM-D]
GPD_SPE_091	GlobalPlatform Technology TEE PP-Module Biometric System v1.0	[PPM-BIO]

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Standard / Specification	Description	Ref
GPD_SPD_142	GlobalPlatform Technology TEE PP-Module Trusted User Interface	[PPM-TUI]
GPD_SPE_090	GlobalPlatform Technology TEE PP-Module Secure Media Path	[PPM-SMP]
GP_PRO_023	GlobalPlatform Technology TEE Certification Process v1.1	[TEE CP]
GPD_GUI_044	GlobalPlatform Technology TEE Evaluation Methodology v1.0	[TEE EM]
GP_TEN_053	GlobalPlatform Technology Cryptographic Algorithm Recommendations v1.0	[CRYPTO]
GPD_TEN_081	GlobalPlatform Technology Cryptography Recommendations for TEE Internal Mechanisms	[TEE CRec]
GPD_SPE_009	GlobalPlatform Technology TEE System Architecture v1.1	[SA]
GPD_SPE_007	GlobalPlatform Technology TEE Client API Specification v1.0	[CAPI]
GPD_EPR_028	GlobalPlatform Technology TEE Client API Specification v1.0 Errata and Precisions v2.0	[CAPI]
GPD_SPE_010	GlobalPlatform Technology TEE Internal Core API Specification v1.2.1	[IAPI]
GPD_SPE_024	GlobalPlatform Technology TEE Secure Element API Specification v1.1.1	[TEE SE]
GPD_SPE_020	GlobalPlatform Technology Trusted User Interface API Specification v1.0	[TUI]
GPD_SPE_025	GlobalPlatform Technology TEE TA Debug Specification v1.0.1	[TA DEBUG]
	GlobalPlatform Technology TEE Initial Configuration Test Suite v2.0.0.2	[ICTS]
…	*Other GlobalPlatform APIs*	…
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]

Table 1-2: Additional References

Reference	Standard / Specification	Ref
…	*Specification of Proprietary API implemented by the TOE*	…
…	*Specification of preinstalled TAs*	…

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

1.4 Terminology and Definitions

Section 1.4 is not mandatory in the ST.

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 author may define key words in this section.

1.4.2 Other Terminology

The ST author 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 author 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

1.6 Revision History

While the document is being developed, the ST author shall record at least the versions that are delivered to third parties, including the laboratory and GlobalPlatform CB.

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

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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	

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

2 Identification

2.1 Security Target Identification

The ST author shall fill-in the identification table Table 2-1.

Table 2-1: ST identification

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

2.2 TOE Type

The ST author shall fill-in the characterization in Table 2-2.

Table 2-2: TOE type

TOE type	
TOE type	*TEE on System-on-Chip or* *TEE on Final Device or* *TEE-part*
Single TOE or Multiple TOEs	*Single/Multiple* *(this information has to match the identification tables below)*

2.3 TOE Identification

The ST author shall provide the identification of the TOE and its components including any pre-installed TAs.

"Reference" stands for a unique identifier including the version number and release date if applicable.

The ST author shall include the hash of the software components as part of the unique identification.

The references are those used in the developer/manufacturer configuration management system(s).

Depending on the TOE type, only one of the following identification tables shall be used.

For a "TEE on SoC" the following table shall be used:

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Table 2-3: TOE identification (TEE on SoC)

TOE identification	
TOE name	Name or N/A
TOE reference	Unique identifier
Developer(s)	Name(s) and address(es)
SoC reference	Unique identifier
ROM code reference	Unique identifier
Boot code reference	Unique identifier
ATF reference	Unique identifier
TEE binary reference	Unique identifier
Pre-installed TA(s) reference(s)	Unique identifier(s)

For TEE on Final Device the following table shall be used:

Table 2-4: TOE identification (TEE on Final Device)

TOE identification	
TOE name	Name or N/A
TOE reference	Unique identifier
Developer(s)	Name(s) and address(es)
Final Device reference	Unique identifier
ROM code reference	Unique identifier
Boot code reference	Unique identifier
ATF reference	Unique identifier
TEE binary reference	Unique identifier
Pre-installed TA(s-reference(s)	Unique identifier(s)

For a TEE-part the following table shall be used:

Table 2-5: TOE identification (TEE-part)

TOE identification	
TOE name	Name or N/A

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

TOE reference	Unique identifier
Developer(s)	Name(s) and address(es)
…	References of the TOE components depending on the scope of the TEE-part

For any of the three types, the following table shall be used for the identification of the pre-installed TAs:

Table 2-6: Pre-installed TAs identification

Pre-installed TA identification	
TA name	Name or N/A
TA reference	Unique identifier
Developer	Name and address
TA binary reference	Unique identifier
Applied Used Guidance	Reference(s) of the TEE guidance that has been used
Description	Purpose of the TA, if there is no guidance referenced why, etc.

2.4 Non-TOE Components Identification

The ST author shall provide the references of the hardware, firmware or software non-TOE components that are required for the operation of the TEE, for instance, external DRAM, or that have some interface with the TOE, for instance, Regular OS, NFC Controller, Fingerprint sensor, etc.

The ST author shall include the hash of the software components as part of the unique identification.

Non-TOE components identification			
Name	**Reference**	**Developer(s)**	**SoC or Device reference**
Commercial name	Unique identifier	Name	List of SoC and/or Device references to which these non-TOE components apply

2.5 Security Guidance Identification

The ST author shall fill-in the following security guidance identification tables applicable to the TOE type.

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Table 2-7: Guidance for integrators

Guidance for TEE integrators	
Document title	
Document reference	
Document version	
Document publication date	
Document status (optional)	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*

Table 2-8: Guidance for TA developers

Guidance for TA developers	
Document title	
Document reference	
Document version	
Document publication date	
Document status (optional)	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*

Table 2-9: Guidance for end users

Guidance for end users	
Document title	
Document reference	
Document version	
Document publication date	
Document status (optional)	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Table 2-10: Guidance for TEE-part integration

TEE-part Integration Guidance	
Document title	
Document reference	
Document version	
Document publication date	
Document status (optional)	*Draft – Final* *Confidential – Restricted – Public* *or any other classification used in your company*
Document author	*Name and company*

2.6 Developers and Manufacturers Identification

The ST author shall fill-in the developer and manufacturer identification table.

Table 2-11: Development and manufacturing sites

Developer/ Manufacturer	Legal Address	Contact	TOE-related sites	Site audits/date
Company name	Address	Name, Title	Sites involved in the development / manufacturing of the TOE	For each site, list of audits performed within 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

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

3 Compliance Claims

3.1 GlobalPlatform API Functional Compliance

The ST author shall fill-in the GlobalPlatform API reference table indicating the version and type of compliance with GlobalPlatform specifications:

- CF (Certified Full functional compliance): means that the TOE 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).
- DF (Declared Full functional compliance): means that the TOE implements an approved version of the API but the compliance has not been qualified by GlobalPlatform.
- DP (Declared Partial functional compliance): means that the TOE partially implements an approved version of the API. The Vendor shall identify the compliant/non-compliant parts of the API.
- NI (Not Implemented): the TOE does not implement the API.

For CF, DF and DP types of compliance, the ST author shall also indicate the reference of the test suite and for CF the reference of the LOQ.

Table 3-1: GlobalPlatform API compliance

API reference	API version	Compliance type	Test suite reference	LOQ reference

3.2 Proprietary API

The ST author shall fill-in the following table with the identification of the non-GlobalPlatform API implemented by the TOE, including the owner (developer) of the specification and indicating whether the API is related to the claimed SFRs or not:

Table 3-2: Proprietary API identification

Reference	Standard / Specification	Version	Developer	SFR-related
reference	*Non-GlobalPlatform API implemented by the TOE*	*Version number*		*Yes/No*

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

3.3 GlobalPlatform Protection Profile Compliance

The ST author shall fill-in the following TEE PP identification table indicating the applicable versions of the TEE PP and PP-Modules for which compliance is claimed. Note that the compliance with TEE PP is mandatory except for TEE-parts.

Reference	GlobalPlatform Technology	V.	Compliance
GPD_SPE_021	TEE Protection Profile		Yes/No
GPT_SPE_140	TEE Time and Rollback PP-Module		*Yes/No*
GPT_SPE_141	TEE Debug PP-Module		*Yes/No*
GPD_SPE_091	TEE Biometric System PP-Module		*Yes/No*
GPD_SPD_142	TEE Trusted User Interface PP-Module		*Yes/No*
GPD_SPE_090	TEE Secure Media Path PP-Module		*Yes/No*
	Other PP-Modules		*Yes/No*

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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, firmware and software components and boundaries, i.e. the architecture and the physical and logical interfaces of the TOE, including the GlobalPlatform and proprietary APIs available to the TAs, 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 all the enabled debug modes.

4.3 Life Cycle

The ST author shall describe the TOE life cycle, in particular the developer(s) and manufacturer(s) that are involved, the unique identifier, the storage root of trust injection steps, and the TOE delivery point.

The following generic description provided in the TEE 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.”

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

5 Security Problem Definition (SPD)

This section defines the security problem in terms of assumptions, threats, and organisational security policies.

For a TEE on SoC or TEE on Final Device evaluation:

- The SPD shall strictly comply with the TEE PP and selected PP-Modules, following the Common Criteria requirements stated in ASE_SPD.
- A reference to the TEE PP and selected PP-Modules is sufficient.

For a TEE-part evaluation:

- The SPD shall be based on the TEE PP and selected PP. However, there may be changes due to the smaller scope of evaluation.
- The ST author shall provide the complete list of assumptions, threats and organisational security policies for the TOE and shall also include a correspondence rationale with the TEE PP and applicable PP-Modules to identify the SPD elements that are changed/unchanged, removed or added.

5.1 Threats

For a TEE on SoC or TEE on Final Device evaluation:

- complete list of threats or inclusion by reference to TEE PP and selected PP-Modules.

For a TEE-part evaluation:

- complete list of threats, based on TEE PP and PP-Modules.

5.2 Assumptions

For a TEE on SoC or TEE on Final Device evaluation:

- complete list of assumptions or inclusion by reference to TEE PP and selected PP-Modules.

For a TEE-part evaluation:

- complete list of assumptions, based on TEE PP and PP-Modules.

5.3 Organisational security policies

For a TEE on SoC or TEE on Final Device evaluation:

- complete list of OSPs or inclusion by reference to TEE PP and selected PP-Modules.

For a TEE-part evaluation:

- complete list of OSPs, based on TEE PP and PP-Modules.

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

6 Security Objectives

This section defines the security objectives for the TOE and for the TOE operational environment.

For a TEE on SoC or TEE on Final Device evaluation:

- The ST shall strictly comply with the TEE PP and selected PP-Modules, following the Common Criteria requirements defined in ASE_OBJ.
- A reference to the TEE PP and selected PP-Modules is sufficient.

For a TEE-part evaluation:

- The objectives shall be based on the TEE PP and selected PP. However, there may be changes due to the smaller scope of evaluation.
- The ST author shall provide the complete list of objectives and shall also include a correspondence rationale with the TEE PP and applicable PP-Modules to identify the objectives that have changed/unchanged, removed or added.

6.1 Security objectives for the TOE

For a TEE on SoC or TEE on Final Device evaluation:

- complete list of objectives for the TOE or inclusion by reference to TEE PP and selected PP-Modules.

For a TEE-part evaluation:

- complete list of objectives for the TOE, based on TEE PP and PP-Modules.

6.2 Security objectives for the TOE operational environment

The ST author shall include an explicit statement of all the security objectives for the TOE operational environment, which must be addressed in the security guidance.

This holds for all types of TOE: TEE on SoC, TEE on Final Device or TEE-part.

Note: It is allowed to refine OEs. For example, OE.INTEGRATION_CONFIGURATION can be refined to cover the protection of an external memory (not in the TOE).

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

7 Security Functional Requirements

The ST author shall include all the Security Functional Requirements (SFR) defined in the TEE PP and applicable PP-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…]

The ST author shall use a police or color of their choice to highlight the TOE-specific instantiations.

The ST author can add “application notes” to explain or clarify the meaning of the SFR in the context of the TOE.

The ST shall contain a section for the SFRs defined in the TEE PP, and optionally as many sections as applicable PP-Modules.

For a TEE on SoC or TEE on Final Device:

- the ST author shall not remove any SFR from the TEE PP and applicable PP-Modules, or modify the fixed text.

For a TEE-part:

- the ST author shall also include a correspondence rationale with the TEE PP and applicable PP-Modules to identify the SFRs that are changed/unchanged, removed or added.

7.1 TEE PP

To be completed with the SFRs from TEE PP v1.3 (or applicable PP).

The instantiation of the cryptographic SFRs (FCS_COP.1) for the internal TSF mechanisms is expected to comply with [TEE CRec].

7.2 PP-Module

As many sections as necessary.

To be completed with the SFRs from TEE PP-Modules (applicable versions).

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

8 Security Assurance Requirements

The ST author shall include the instantiation of AVA_VAN_AP.3 for the parts of the implementation representation that are available to the evaluator. These parts must be uniquely identified as TOE components in the identification chapter of the ST.

Remark: for a 3-month full TEE evaluation, the instantiation of AVA_VAN_AP.3 must cover all the firmware and software that contributes to the security functionality, including the TEE initialization code, the TEE firmware (Trusted OS, communication agent with REE, drivers), and also the code of the TA(s) that belong to the TOE (if any).

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

9 Functional Description

The ST author shall provide a functional description that explains how the TOE fulfills the SFRs, in particular the role of the hardware, firmware and software components and security mechanisms in the implementation of the SFRs.

The ST author shall provide an explanation for each SFR. References to external documentation available to the laboratory and to GP CB are accepted.

Copyright © 2016-2021 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.