GlobalPlatform Technology

SESIP Profile for WPC Qi Secure Storage Subsystem

Version 0.0.0.15

Public Review

February 2024

Document Reference: GPT_SPE_153

Copyright © 2024 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 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. This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

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.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

Contents

1 Introduction 5
1.1 Audience 6
1.2 IPR Disclaimer 6
1.3 References 6
1.4 Terminology and Definitions 7
1.5 Abbreviations 7
1.6 Revision History 8
2 SESIP References 9
2.1 SESIP Profile Reference 9
2.2 Platform Reference 9
2.3 Guidance Documents 9
3 Platform Component Functional Overview and Description 10
3.1 SSS Security Features and Scope 11
3.2 Physical Scope 12
3.3 Logical Scope 12
3.4 Life Cycle 13
3.5 Non-TOE Hardware/Software/Firmware 13
4 Security Objectives for the Operational Environment 14
5 Security Requirements and Implementation 15
5.1 Security Assurance Requirements 15
5.1.1 Flaw Reporting Procedure (ALC_FLR.2) 15
5.2 Security Functional Requirements 16
5.2.1 Identification and Attestation of Platforms and Applications 16
5.2.1.1 Verification of Platform Identity 16
5.2.1.2 Verification of Platform Instance Identity 16
5.2.1.3 Secure Initialization of Platform 17
5.2.1.4 Attestation of Platform Genuineness 17
5.2.2 Product Lifecycle 18
5.2.2.1 Secure Update of Platform 18
5.2.3 Compliance Functionality 18
5.2.3.1 Secure Debugging 18
5.2.4 Cryptographic functionality 19
5.2.4.1 Cryptographic Operation 19
5.2.4.2 Cryptographic Key Generation 19
5.2.4.3 Cryptographic Random Number Generation 20
5.2.4.4 Cryptographic KeyStore 20
5.2.5 Limited Physical Attacker Resistance 20
5.3 Trust Provisioning Package 21

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

Tables

Table 1-1: Normative References 6
Table 1-2: Terminology and Definitions 7
Table 1-3: Abbreviations 7
Table 1-4: Revision History 8
Table 2-1: SESIP Profile Reference 9
Table 2-2: Platform Reference 9
Table 2-3: Guidance Documents 9
Table 3-1: Hardware Components and Interfaces of the TOE 12
Table 3-2: Software Components and Interfaces of the TOE 12

Figures

Figure 1-1: Examples of Qi Power Transmitters and Receivers 5
Figure 3-1: TOE Scope Representation Example 11

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

1 INTRODUCTION

Qi (pronounced “chee”) is the world’s de facto wireless charging standard for providing 5-15 watts of power to small personal electronics. Though it is primarily used to charge smartphones, the standard can also apply and easily be used to provide power for a growing number of consumer devices. With more than 3,700 Qi-Certified product types on the market today, Qi delivers a positive and safe wireless charging experience. The Wireless Power Consortium (WPC) and its 400+ member companies are committed to continuing to grow this market by delivering differentiated and affordable products.

Secure Storage Subsystems (SSS) are essential elements of security for the WPC ecosystem embedded within a power transmitter, ensuring the authentication and genuineness of power transmitter to power receivers. Typical power transmitters are phone chargers such as automotive or standalone consumer ones.

Figure 1-1: Examples of Qi Power Transmitters and Receivers

This SESIP Profile (SP) describes a generic SSS module that may be used in various wireless charging use cases. It describes the essential security requirements as described in the Qi authentication specification [WPC] & [WPC2] that defines the SSS and its core security features and functionalities.

If a product is certified compliant to this SESIP Profile, the Qi ecosystem can rely upon these security features and upon the security assurance provided that they follow user guidance documentation associated to the certified product.

This SESIP Profile contains the following guidance paragraphs:

- AN: Application Note shall be considered and followed for Security Target (ST) writing
- INFO: Additional context information

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the “License”). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

1.1 Audience

This document is intended primarily for the use of all stakeholders involved in the security evaluations of the SSS module, including developers of the Qi Authentication applet basing their own product on evaluated SSS.

The Qi ecosystem, including but not limited to Qi Applet Developers, regulatory authorities, organizations and schemes using peer assessment, accreditation bodies, end customers and others have the ability to use this document in confirming, validating or recognizing the security level of the SSS platform.

The use of this document will allow harmonization and comparability between SSS security evaluations. The acceptance of results between schemes is facilitated if laboratories conform to this document.

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://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

The table below lists references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: Normative References

Standard / Specification	Description	Ref
GP_FST_070	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP)	[SESIP]
WPC	Qi Specification Authentication 1.3 Qi Specification Authentication 1.3.1 Qi Specification Authentication 1.3.2 Qi Specification Authentication 2.0	[WPC]
WPC	WPC Agreement for Manufacturer CA Service Provider	[WPC2]

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

1.4 Terminology and Definitions

Selected terms used in this document are included in Table 1-2. Additional terms are defined in [SESIP].

Table 1-2: Terminology and Definitions

Term	Definition
Power Receiver	Device receiving power from the Power Transmitter, leveraging the Qi Authentication protocol to identify the Power Transmitter
Power Transmitter	Device providing power to the Power Receiver. Power Transmitter embeds the SSS
Secure Storage Subsystem (SSS)	A tamper resistant subsystem that protects one or more cryptographic key values against exposure outside that subsystem

1.5 Abbreviations

Table 1-3: Abbreviations

Abbreviation	Meaning
RoT	Root of Trust
SAR	Security Assurance Requirement
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirement
SP	SESIP Profile
SSS	Secure Storage Subsystem
ST	Security Target
TOE	Target Of Evaluation
WPC	Wireless Power Consortium

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and clarifications; all non-trivial changes are indicated, often with revision marks.

Table 1-4: Revision History

Date	Version	Description
May 2023	0.8	Transfer from NXP
July 2023	0.0.0.9	Committee Review
Sept 2023	0.0.0.10	Updated SFR to align with new SESIP version 1.2
Sept 2023	0.0.0.11	Member Review
Oct 2023	0.0.0.14	Member Review Update
Feb 2024	0.0.0.15	Public Review
TBD	v1.0	Public Release

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

2 SESIP References

2.1 SESIP Profile Reference

Table 2-1: SESIP Profile Reference

Item	Description
SP Name	SESIP Profile for WPC Qi Secure Storage Subsystem
SP Version	Version 0.0.0.11
TOE Type	Secure Storage Subsystem
Assurance claim	SESIP Assurance level 2 with limited physical attacker resistance

2.2 Platform Reference

Table 2-2: Platform Reference

Item	Description
TOE Name	<TBD>
TOE Version	<TBD>
TOE Identification	<TBD>
TOE type	<TBD>

2.3 Guidance Documents

Table 2-3: Guidance Documents

Item	Name	Version
<Ref>	<TBD>	<TBD>

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

3 Platform Component Functional Overview and Description

The scope of the Secure Storage Subsystem (see next chapters for more information) is defined as follow:

- The **physical scope** = SSS processing unit
- The **logical scope** = includes the SSS firmware

Note = Additional hardware parts included in the platform together with their firmware, as well as higher software layers (e.g. software Root of Trust services, software platform parts, or final applications) are outside of the evaluation scope.

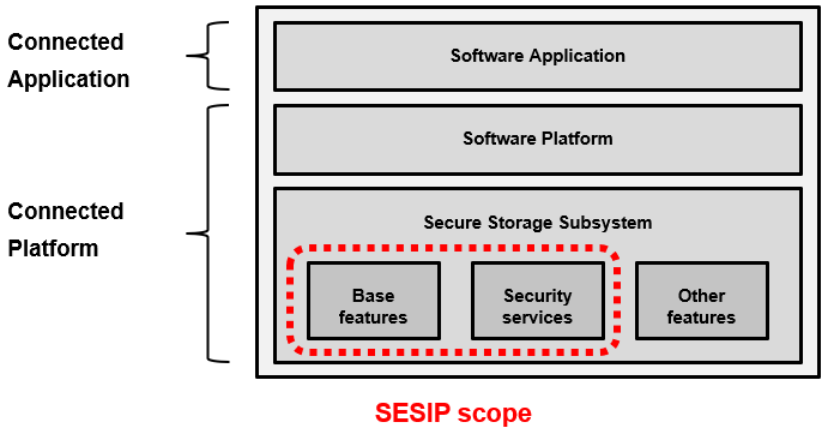
Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

3.1 SSS Security Features and Scope

Figure 3-1 illustrates the SESIP protection Profile for the SSS, including:

- **"Base features" and "Security Services" are within the base evaluation scope** and are hence covered by this protection profile
- **"Other features" are optional part of the evaluation** and can be added to the scope

Figure 3-1: TOE Scope Representation Example



The TOE security features (see section 5 for further details) of the TOE are:

Component
Base Feature
Flaw reporting procedure
Security Services
Identification and Attestation of Platforms and Applications
Product Lifecycle
Cryptographic Functionality
Limited Physical Attacker Resistance
Trust Provisioning

AN The Security Target shall precisely describe the physical and logical scope of the TOE, and provide all necessary details required to identify the libraries, drivers, and other modules that are used, together with their versions and any other relevant information. Additional details about the security features supported by the SSS must be described.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

3.2 Physical Scope

The TOE provides the following hardware components and interfaces:[1]

Table 3-1: Hardware Components and Interfaces of the TOE

Component/Interface	Description	Identification
Communications ports	*e.g. UART, I2C, SPI, <TBD>*	
Memories	*e.g. Flash*	
Human Interface	*e.g. GPIO*	
Timers	*e.g. Timer/PWM outputs, Input capture*	
Analog Interface	*e.g. ADC inputs, DAC outputs*	
Debug port	*JTAG*	
…		

AN The Security Target writer shall update the table above with the listing of all hardware components and interfaces involved in SSS. The table above provides examples of hardware components and interfaces.

3.3 Logical Scope

The TOE provides the following software components and interfaces:[2]

Table 3-2: Software Components and Interfaces of the TOE

Component/Interface	Description	Identification / Version
Bootloader	*ROM image*	
Firmware	*FLASH image*	
Crypto Library	*FLASH image*	
APIs	*APIs*	
...		

AN The Security Target writer shall update the table above with the listing of Software components and Interfaces of the TOE involved in SSS. The table above provides typical examples of the logical scope.

[1] Hardware interfaces are hardware modules and physical ports exposed to the environment.

[2] Software interfaces are the logical features exposed to the environment (including firmware).

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

3.4 Life Cycle

AN The Security Target shall describe the life cycle of the SSS under evaluation.

The description must present an overview of the main lifecycle phases from hardware and software design to the product end-of-life; for each phase, all possible SSS state(s) must be identified; how transitions between those states are secured must also be explained.

The description must include how the provisioning is performed (directly in the ST or referencing the appropriate guidance document).

No example is given as this section is usually implementation specific.

3.5 Non-TOE Hardware/Software/Firmware

AN The Security Target shall describe if the TOE is supplied with existing apps, Application Root of Trust Services or other components. If the TOE is supplied with other components these shall be listed here.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

4 Security Objectives for the Operational Environment

For the SSS platform to fulfil its security requirements, the operational environment (technical or procedural) must implement the following objectives:

ID	Description
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the TOE are subject to secure key management procedures
UNIQUE_ID	The integrity and uniqueness of the unique identification of the TOE must be provided by the TOE user during the personalization stage
PRODUCT_USAGE	The device manufacturer is expected to respect integration and usage manual and security guidance described in the <*Reference*>

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

5 Security Requirements and Implementation

AN In this chapter, the Security Target shall define the Security Assurance Level claimed and the list of Security Functional Requirements in the scope of the evaluation; this list must be compliant with the security features listed in the product description.

5.1 Security Assurance Requirements

The minimum claimed assurance requirements package is **SESIP2** as defined in [SESIP].

5.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to report flaws and generate and distribute any needed updates, the developer has defined the following procedure:

AN The Security Target shall describe the procedure, including where flaws and security incidents can be reported (website and/or email address), how the reported flaws are handled in a timely manner, and how an application developer/end-user can get informed of the update. If the “Secure Update of the platform” SFR is removed, a strong argumentation shall be provided detailing why the platform is not worth getting an update. However, the process to receive the reports of flaws and handling them in a timely manner needs to be described in any case.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the “License”). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

5.2 Security Functional Requirements

5.2.1 Identification and Attestation of Platforms and Applications

5.2.1.1 Verification of Platform Identity

Requirement

The platform provides a unique identification of itself, including all its parts and their versions.

Refinement

Assets and protections related to this SFRs are:

Asset	Protection required	Comments
SSS module Platform Identity	Integrity	The modification of the platform id is impacting the user configuration management.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

For example, the platform can be identified by data stored in ROM/NVM at manufacturing time including the SSS module name, type and version, invokable through an API. Note that this must allow to uniquely identify the model and version of hardware, firmware and software, either directly through the invocation or by a global name and version corresponding to a unique set of hardware, firmware and software provided into guidelines and linkable to configuration management information.

5.2.1.2 Verification of Platform Instance Identity

Requirement

The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

Refinement

Assets and protections related to this SFRs are:

Asset	Protection required	Comments
SSS module Platform Identity	Integrity	The modification of the platform instance id may impact the Qi certificate

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

For example, the specific instance of a platform can be identified by a serial number or UUID through an API.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

5.2.1.3 Secure Initialization of Platform

Requirement

The platform ensures its integrity and authenticity during platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to **a state where no other operation except optionally Secure Update of Platform, Secure Debugging can be performed**.

Refinement

If the initialization fails, restarts of the device to reinitiate boot sequence might be done. If unsuccessful, recovery using the update mechanism may be performed. All other functionalities must not be available. The application may be used to facilitate this update but must not provide any other functionality until the authenticity and integrity of the platform is reestablished.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

Any guidance for the application on this must be explicitly mentioned as a Security Objectives for the operational environment, with explicit reference to where this guidance is provided.

For example, the secure initialization can be based on a secure boot based on a chain of signature verifications ensuring the integrity and authenticity of the Firmware; and any issue in this process leads to a reset.

5.2.1.4 Attestation of Platform Genuineness

Requirement

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity” in a way that ensures that the platform has not been cloned or changed without detection.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the “License”). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

5.2.2 Product Lifecycle

5.2.2.1 Secure Update of Platform

Requirement

The platform can be updated to a newer version in the field such that the confidentiality, integrity, and authenticity of the platform is maintained.

Refinement

Assets and protections related to this SFRs are:

Asset	Protection required	Comments
SSS module Firmware and Software	Integrity, authenticity	Firmware running on SSS module playing a central role in the secure initialization of the platform. Modification of this asset would allow the attacker bypassing the device integrity and extract Qi private keys
SSS module Firmware and Software	Monotonic	Firmware and software can only be updated to a version greater or equal to the current version.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

For example, the secure update of the firmware/software can be part of the secure initialization process with the authenticity and version verification and ensuring no rollback of the firmware/software.

5.2.3 Compliance Functionality

5.2.3.1 Secure Debugging

Requirement

The platform only provides ***<list of endpoints>*** authenticated as specified in ***<specification>*** with debug functionality.

The platform ensures that all user data stored, with the exception of ***<list of exceptions>***, is made unavailable.

Refinement

All assets defined in other Security Functional Requirements and accessible through the Secure Debugging mechanism shall be protected against unauthorized access.

For debug functionality authentication, device specific credentials shall be used.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

5.2.4 Cryptographic functionality

5.2.4.1 Cryptographic Operation

Requirement

The platform provides ***<Operations, see table below>*** functionality with ***<Algorithm, see table below>*** as specified in ***<Specification, see table below>*** for key lengths ***<Key lengths, see table below>*** and modes ***<Modes, see table below>***.

Operations	Algorithm	Specification	Key lengths / message lengths	Modes
Signature generation	ECDSA P256	FIPS 186-4	256	NA
Hash certificate	SHA-256	FIPS 180-4	256	NA

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

5.2.4.2 Cryptographic Key Generation

Requirement

The platform provides a way to generate cryptographic keys for use in ***<Operations, see table below>*** as specified in ***<Algorithm & specification, see table below>*** for key lengths ***<Key lengths, see table below>***.

Operations	Algorithm	Specification	Key lengths
ECC key generation	ECDSA P256	FIPS 186-4	256

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

5.2.4.3 Cryptographic Random Number Generation

Requirement

The platform provides a way based on **an entropy source as described below** to generate random numbers to as specified in **NIST SP 800-90 A in the following list: <Hash_DRBG (any), HMAC_DRBG (any) and/or CTR_DRBG (AES)>.**.

Entropy source details: source that accumulates entropy from <noise source> with a minimum of <selection: 128 bits, 256 bits> of entropy at least equal to the greatest security strength (according to NIST 800-57) of the keys and hashes that it will generate. An entropy source that adheres to NIST 800-90B or AIS 20/31 classes of DRG.3, or DRG.4, or PTG.3, each seeded with a PTG.2 noise source, is sufficient.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

5.2.4.4 Cryptographic KeyStore

Requirement

The platform provides a way to store ***<list of assets, such as cryptographic keys and passwords, see table below>*** such that not even the application can compromise the ***<confidentiality, integrity, and authenticity, see table below>*** of this data. This data can be used for the cryptographic operations ***<list of operations, see table below>***.

Assets	Security property	List of operations
Qi private key ECDSA-P256	Authenticity, integrity and confidentiality	Qi authentication support of the Power Transmitter by the Power Receiver

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

5.2.5 Limited Physical Attacker Resistance

Requirement

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises the requirements claimed as part of the SFR Cryptographic Operation.

AN The Security Target must describe here how the specific SSS module target of the evaluation is fulfilling the requirement and the associated refinements if any.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

5.3 Trust Provisioning Package

INFO This package describes the security claims concerning the trust provisioning handling by the environment through secure processes, and platform in case some supporting features platform side are needed.

Requirement

The Trust Provisioning system ensures the secure management in a trusted environment of **Qi Authentication keys** and its loading into the platform for the following use cases: **Authentication compliant with Qi Authentication**.

Both the trusted environment and the platform protect **access, confidentiality, integrity** of provisioned data.

Rationale

AN The Security Target shall provide a high level description of how the requirement is implemented by the developer of the platform under evaluation and the platform itself. For instance, data injected could be a key used then for further key injection in an untrusted environment e.g. a test center, OEM manufacture, in the field, etc.

INFO As part of the evaluation, the developer must provide documentation of the secure process implemented by the trusted environment to ensure the secure management and loading.

The evaluation must assess the security of the secure process put in place by the trusted environment based on the developer documentation and potentially on verifications performed on the platform (e.g. generation of a hash). No audit is required. The evaluation must also assess the security of the protections implemented by the platform to ensure the protections selected for the provisioned data.

At minimum the following must be provided and evaluated:

- Secure management description e.g. key generation, key storage, etc.
- Secure loading description e.g. cryptographic algorithm
- Type of data to be loaded by the Trust Provisioning System; in particular if data is a key, key length must be specified.
- Use cases description e.g. OEM secure loading of their own assets.
- Protections descriptions of the loaded data by the platform.

Reference to guideline for the assessment of this activity can be added.

Copyright © 2024 GlobalPlatform, Inc. All Rights Reserved.
This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.