GlobalPlatform®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology

Cryptography Recommendations for TEE Internal Mechanisms

Version 0.0.0.8

Public Review

November 2020

Document Reference: GPD_TEN_081

Copyright © 2018-2020 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. This document is currently in draft form, and the technology provided or described herein may be subject to updates, revisions, extensions, review, and enhancement by GlobalPlatform or its Committees or Working Groups. Prior to publication of this document by GlobalPlatform, neither Members nor third parties have any right to use this document for anything other than review and study purposes. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement 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 © 2018-2020 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

Copyright © 2018-2020 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.

Tables

Copyright © 2018-2020 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

Cryptography is an important pillar of a digital service's security and impacts the application, the Secure Component, and the related management systems. In order to help the market to anticipate required migration, GlobalPlatform has decided to provide regular cryptography recommendations and defined transition periods that are applicable to TEE internal security mechanisms.

1.1 Audience

This document provides guidance for TEE Implementers, whether involved with TEE boot or with providing TEE run-time services.

TA writers may consult this document for insight into the cryptographic aspect of the security of the environment they are using.

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 tables below list references applicable to this document. 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
GPD_SPE_021	GlobalPlatform Technology TEE Protection Profile v1.2.1 or above	[TEE PP]
GP_TEN_053	GlobalPlatform Technology Cryptographic Algorithm Recommendations	[Crypto Rec]

Table 1-2: Informative References

Standard / Specification	Description	Ref
BSI-CC-PP-0084	Common Criteria Protection Profile Security IC Platform Protection Profile with Augmentation Packages	[PP-0084]
OMTP ATE TR1	Open Mobile Terminal Platform (OMTP) Advanced Trusted Environment TR1 v1.1	[OMTP-TR1]

Copyright © 2018-2020 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

Table 1-3: Terminology and Definitions

Term	Definition
Client Application (CA)	An application running outside of the Trusted Execution Environment (TEE) making use of the TEE Client API (**Error! Reference source not found.**) to access facilities provided by Trusted Applications inside the TEE. Contrast **Error! Reference source not found.**.
Execution Environment (EE)	An environment that hosts and executes software. This could be an REE such as Android, Linux, or Windows; it could be an SE or a GlobalPlatform TEE; or it could be an abstract platform such as a web browser.
Regular Execution Environment (REE)	An Execution Environment comprising at least one Regular OS and all other components of the device (SoCs, other discrete components, firmware, and software) which execute, host, and support the Regular OS (excluding any Secure Components included in the device). From the viewpoint of a Secure Component, everything in the REE is considered untrusted, though from the Regular OS point of view there may be internal trust structures. (Formerly referred to as a *Rich Execution Environment (REE)*.) Contrast *Trusted Execution Environment (TEE)*.
Regular OS	An OS executing in a Regular Execution Environment. May be anything from a large OS such as Linux down to a minimal set of statically linked libraries providing services such as a TCP/IP stack. (Formerly referred to as a *Rich OS* or *Device OS*.) Contrast *Trusted OS*.
Secure Element (SE)	A tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. May exist in any form factor, such as embedded or integrated SE, SIM/UICC, smart card, smart microSD, etc.
Tamper-resistant secure hardware	Hardware designed to isolate and protect embedded software and data by implementing appropriate security measures. The hardware and embedded software meet the requirements of the latest Security IC Platform Protection Profile ([PP-0084]) including resistance to physical tampering scenarios described in that Protection Profile.

Copyright © 2018-2020 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.

Term	Definition
Trusted Application (TA)	An application running inside the Trusted Execution Environment that provides security related functionality to Client Applications outside of the TEE or to other Trusted Applications inside the TEE. Contrast *Client Application (CA)*.
Trusted Execution Environment (TEE)	An Execution Environment that runs alongside but isolated from an REE. A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets against a set of defined threats which include general software attacks as well as some hardware attacks, and defines rigid safeguards as to data and functions that a program can access. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly. Contrast *Regular Execution Environment (REE)*.
Trusted OS	An OS executing in a Secure Component. Contrast *Regular OS*.
Trusted Storage	In GlobalPlatform TEE documents, storage that is protected to at least the robustness level defined for OMTP Secure Storage (in [OMTP-TR1] section 5). It is protected either by the hardware of the TEE, or cryptographically by keys held in the TEE. If keys are used, they are at least of the strength used to instantiate the TEE. A GlobalPlatform TEE Trusted Storage is not considered hardware tamper resistant to the levels achieved by Secure Elements.

1.5 Abbreviations and Notations

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	Execution Environment
REE	Rich Execution Environment
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SE	Secure Element
SHA	Secure Hash Algorithm
TA	Trusted Application
TEE	Trusted Execution Environment
TP	Transition Periods

Copyright © 2018-2020 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.

1.6 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 precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-5: Revision History

Date	Version	Description
April 2018	0.0.0.2	Committee Review
July 2019	0.0.0.7	Member Review
November 2020	0.0.0.8	Public Review
TBD	1.0	Public Release

Copyright © 2018-2020 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 Cryptography Recommendations for TEE Internal Mechanisms

2.1 Scope

GlobalPlatform has issued cryptography recommendations and defined transition periods that are applicable to TEE internal security mechanisms, such as secure initialization, Trusted Storage, Trusted Application management, and debug administration, whenever they rely solely on cryptographic protection.

Recommendations reflect the minimum security level that is approved for a GlobalPlatform-certified TEE compliant with TEE Protection Profile ([TEE PP]).

Some algorithms and key sizes that do not reach the recommended security level may be accepted during a transition period.

The recommendations and transition periods do not apply to cryptographic functionality directly exposed by the Trusted OS to Trusted Applications, which are responsible for the mechanisms they are using.

For complete information about GlobalPlatform cryptographic recommendations, see Cryptographic Algorithm Recommendations ([Crypto Rec]).

2.2 Validity

Recommendations take effect immediately unless otherwise specified.

Each version of this technical note may specify transition periods during which specific exceptions to the recommendations may pass certification testing.

GlobalPlatform will revise and publish cryptography recommendations and transition periods regularly and following adversary events that could impact the security of GlobalPlatform-certified TEE products.

2.3 Recommendations (R)

GlobalPlatform recommendations on cryptographic strength are aligned with international standards[1] guidelines that advocate a 128-bit security level:

(R1) Symmetric cryptography: At least equivalent to the combination of a symmetric algorithm and mode of operation both recommended (Recommendation level: REC or higher) from [Crypto Rec],

(R2) Hash functions: At least equivalent to a hash function recommended (Recommendation level: REC or higher) from [Crypto Rec],

(R3) Asymmetric cryptography: At least equivalent to an asymmetric algorithm recommended (Recommendation level: REC or higher) from [Crypto Rec].

[1] For instance, NIST SP 800 Series and SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.

Copyright © 2018-2020 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.

2.4 Transition Periods (TP)

Currently one transition period is defined:

(TP1) TEE internal security mechanisms may continue to use RSA/DSA 2048 (considered to have a 112-bit security level) through 31 December 2023.

Note: This recommendation is aligned for RSA with the recommendation of level LEG from [Crypto Rec],

2.5 Observations

The recommendations are believed to be well-aligned with the level of attack potential defined in TEE Protection Profile ([TEE PP]) and might change according to future evolutions of the attack potential. However, the current recommendations are not expected to change in the near future.

With regard to RSA/DSA, developers of implementations intended for long product lifetime should consider moving those implementations to the recommended level (R) as soon as possible.

As a general design principle, TEE implementations SHOULD be able to upgrade the security of their internal mechanisms during product life (e.g. by supporting several key lengths or TEE firmware upgrades to versions with higher cryptographic strengths).

Copyright © 2018-2020 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.