GlobalPlatform®
The standard for
secure digital services
and devices

Certificate of Security Evaluation

Xuantie TEE version 1.0

Certification Number:	GP-TEE-2024/01	**Product Name:**	Xuantie TEE version 1.0
Issuance Date:	2024.04.04	**Trusted OS / Developer:**	Xuantie TEE version 1.0 / T-Head
Sponsor:	T-Head (Shanghai) Semiconductor Technology Co., Ltd.	**SoC / Developer:**	TH1520 / T-Head
Protection Profile:	TEE PP v1.3 (Core TEE PP)	**Product Type:**	□ TEE on Final Device ☑ TEE on SoC □ TEE partial scope: □ HW/SW □ HW □ SW
PP-Modules:	None		
Certification Type:	☑ Full □ Restricted	**Evaluation Type:**	☑ Full □ Delta □ Fast-track
Certification Report:	GP-TEE-2024/01-CR v1.0	**Security Evaluation Lab:**	DPLS Lab (Beijing, China)

This GlobalPlatform Security Evaluation Product Certificate ("Certificate") remains valid only while the version of the product specified above is posted on the GlobalPlatform website, and means only that such product version has demonstrated sufficient conformance with applicable GlobalPlatform TEE Security Requirements, determined by a GlobalPlatform-accredited third-party evaluation laboratory. This Certificate applies only to the product version specified, does not constitute an endorsement or warranty by GlobalPlatform, and is subject to the additional terms, conditions and restrictions set forth in the attached GlobalPlatform TEE Security Scheme Certification Report.

GlobalPlatform, Inc.

Gil Bernabeu, Certification Director

GlobalPlatform®
Security Certified
TEE

The standard for
secure digital services
and devices

GlobalPlatform TEE Security Scheme

Certification Report

GP-TEE-2024/01-CR-1.0

Issue date:	2024.04.04
Product:	Xuantie TEE v1.0
Sponsor and Developer:	T-Head (Shanghai) Semiconductor Technology Co., Ltd. Building A2, Alibaba Shanghai R&D center, No.55 Chuanhe Road, Shanghai, China
Laboratory:	BEIJING ZHIHUIYUNCE (DPLS LAB) EQUIPMENT TECHNOLOGY CO., LTD. Room 701, building 7 No. 98, Lianshi Lake West Road, MentougouDistrict, Beijing, China 102308
Conformance:	☑ TEE PP v1.3 (Core TEE PP)
Product Type:	☐ TEE on Final Device ☑ TEE on SoC ☐ TEE partial scope: ☐ HW/SW ☐ HW ☐ SW
Evaluation Type:	☑ Full ☐ Delta ☐ Fast-track
Certification Type:	☑ Full ☐ Restricted

NOTICE

GlobalPlatform, Inc. (“GlobalPlatform”) has received the request of the above listed sponsor(s) (collectively, “Sponsor”) for security certification of the above referenced product version (“Product”). After assessing such request and the security evaluation reports submitted therewith, GlobalPlatform has found reasonable evidence that the Product sufficiently conforms to the GlobalPlatform TEE Security Requirements.

GlobalPlatform therefore (a) issues this Certification Report and accompanying Product (Restricted) Certificate for the Product (collectively, the “Certification”), subject to the terms, conditions and restrictions set forth herein, and (b) agrees to include the name of the Sponsor, and name of the developer(s) above listed upon request, as well as the Product on GlobalPlatform’s website in accordance with applicable policies and procedures. Because this Certification is subject to limitations, including those specified herein and certain events of termination, Sponsor and any third parties should confirm that such Certification is current and has not been terminated by referring to the list of certified products published on the GlobalPlatform website (www.globalplatform.org).

CONDITIONS

This Certification (a) only applies to the above referenced Product version, (b) is conditioned upon all necessary agreements having been executed in accordance with GlobalPlatform policy and satisfaction of the requirements specified therein, and shall be effective only if such agreements and requirements satisfaction continue to be in full force and effect, (c) is subject to all terms, conditions and restrictions noted herein, (d) is issued solely to the submitting Sponsor and solely in connection with the Product and (d) may not be assigned, transferred or sublicensed, either directly or indirectly, by operation of law or otherwise.

Only a product with valid GlobalPlatform Certification may claim to be a ‘GlobalPlatform Certified Product’.

GlobalPlatform may revoke this Certification at any time in its sole discretion, pursuant to the terms of this Certificate Report and the GlobalPlatform TEE Security Certification Process and related agreements. Accordingly, no third party should rely solely on this Certification, and continued effectiveness of this Certification should be confirmed against the applicable list of certified Products on the GlobalPlatform website. Even though GlobalPlatform has certified the Product, the Sponsor shall be responsible for compliance with all applicable specifications and Security Requirements and for all liabilities resulting from the use or sale of the Product.

In addition to GlobalPlatform’s rights to now communicate this Certification, upon the Sponsor’s authorization, you may now communicate that the Product listed above is GlobalPlatform certified (using the same or similar terms); provided, however, that (a) you also communicate all terms, conditions and restrictions set forth herein, (b) when identifying that the Product has been GlobalPlatform certified (using the same or similar terms), you provide specific details identifying the product and version that has been certified and not release a general statement implying that all of your products (or product versions that have not been certified) are certified, (c) your communication in no way suggests that by using your products that a vendor will be guaranteed by GlobalPlatform, (d) your communication in no way implies that you are a preferred product vendor of GlobalPlatform or that you or the Product are endorsed by GlobalPlatform, and (e) all written communications referring to GlobalPlatform’s certification shall contain the following legend:

“GlobalPlatform issuance of a certificate for a given product means only that the product has been evaluated in accordance and for sufficient conformance with the then current version of the GlobalPlatform TEE Security Requirements, as of the date of evaluation. GlobalPlatform’s certificate is not in any way an endorsement or warranty regarding the completeness of the security evaluation process or the security, functionality, quality or performance of any particular product or service. GlobalPlatform does not warrant any products or services provided by third parties, including, but not limited to, the producer or vendor of that product and GlobalPlatform certification does not under any circumstances include or imply any product warranties from GlobalPlatform, including, without limitation, any implied warranties of merchantability, fitness for purpose, or non-infringement, all of which are expressly disclaimed by GlobalPlatform. To the extent provided at all, all representations, warranties, rights and remedies regarding products and services which have received GlobalPlatform certification shall be provided by the party providing such products or services, and not by GlobalPlatform, and GlobalPlatform accepts no liability whatsoever in connection therewith.”

Contents

Tables

1 Executive Summary

This document constitutes the Certification Report for the evaluation of the product *Xuantie TEE v1.0,* developed by T-Head (Shanghai) Semiconductor Technology (T-Head), registered under number GP230009.

The type of TOE is a *Trusted Execution Environment (TEE) on SoC.*

The evaluation has been performed by accredited laboratory DPLS LAB in Beijing (China). The following documents constitute the basis for this evaluation: *Xuantie TEE Security Target v1.1.11, ref STG90002*, *Guidance for SoC integrators v1.0, ref. STG90003*, *Guidance for TA developers v1.0, ref. STG90004* and *Guidance for TEE final users v1.0, ref. STG90005*.

The evaluation determined that the product, as identified in this report, meets GlobalPlatform TEE security functional requirements stated in the security target at the assurance level AVA_VAN_AP.3 and that the guidance addresses all the objectives for the TOE environment defined in the security target and further recommendations from the evaluation. The results of the evaluation are presented in the technical evaluation report *Xuantie TEE Detailed Technical Evaluation Report, version 3.1.*

The certification determined that the evaluation has been performed in conformance with *GlobalPlatform TEE Protection Profile v1.3* and *TEE Evaluation Methodology v1.2*. The certificate is valid provided all the usage restrictions defined in section 4.1 are fulfilled.

2 Product Information

2.1 Identification

Table 2-1 provides the identification of the Product or Target of Evaluation (TOE).

Table 2-1: Product identification

Product identification	
Product Name	Xuantie TEE v1.0
Developer	T-Head (Shanghai) Semiconductor Technology Co., Ltd.
Product Type	TEE on SoC

Table 2-2 provides the identification of the components of the TOE.

Table 2-2: TOE components identification

TOE components identification		**Developer**
SoC reference	TH1520	T-Head
Hardware reference	Light 100P Checksum: 9389950efd456429c85061e0afbc6067ee60567c3180fc1b3d1f306fbb114b16	T-Head
ROM code	BootROM version 1.5 Checksum: 81791debdd9f31de8287eb5ced6e252eceb0e5aa4b7dc97d70af86aa87a25cbd	T-Head
Boot code	Bootloader version 1.0 Checksum: d577d49c033290e84788bee52f85be6e8149d20f3dafa40f73e89dad1a1579ce	T-Head
ATF	Trust firmware version 1.0 Checksum: d3338c9aa2bd87387ec0fb5497947dabd06513d957c7726177c82a97d1c85445	T-Head
TEE binary	TEE binary version 1.0 Checksum: 71723a20ec08f39e5ecdacd88fd3f8c751548878932bcaf12ae84dfec2ddded6	T-Head
Pre-installed TAs	None	T-Head

2.2 Documentation

The Product documentation consists of the security target and guidance documentation for integrators, application developers, and final users:

- [ST] *Xuantie TEE Security Target v1.1.11, ref. STG90002;*

- [INTEGR_GUIDE] *Guidance for SoC integrators v1.0, ref. STG90003;*
- [DEV_GUIDE] *Guidance for TA developers v1.0, ref. STG90004;*
- [FINAL_GUIDE] *Guidance for TEE final users v1.0, ref. STG90005.*

2.3 Architecture

The hardware architecture of the TOE consists of:

- TH1520, which is a RISC-V C910 Processor with security extension;
- Internal and external physical memories;
- AES and RSA crypto accelerators;
- Random number generator (TRNG for physical source and DRBG using NIST SP800-90A approved algorithm);
- Connections between the processing unit(s) and the hardware resources: AXI-based bus some of which are accessible only from the Secure World through the Xuantie Trusted OS, e.g. JTAG.

The firmware and software architecture of the TOE consists of ROM boot code, Pre-loader, ATF, and T-Head's Secure OS Xuantie TEE on TH1520.

The TOE provides the following software interfaces:

- A proprietary communication interface with the REE;
- A proprietary low-level interface for TA-TEE and TA-TA communication;
- GlobalPlatform API (see Table 2-3);
- Proprietary APIs (see Table 2-4).

Note: The TOE does not include the REE which consists essentially of the regular OS and the applications running on top. The TOE does not include any peripheral device.

The TOE implements the GlobalPlatform API listed in Table 2-3, for which T-Head declares functional compliance in the security target.

Table 2-3: GlobalPlatform API

Reference	Declarative Full Compliance	Version
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

The TOE also implements the Proprietary API listed in Table 2-4, developed by T-Head:

Table 2-4: Proprietary API

Reference	Developer	Version	Content
[C API]	T-Head	1.0	Proprietary_API_01 to _033

2.4 Life cycle

The TOE life cycle is split in 5 development and manufacturing phases and a final end-user phase:

- [T-Head] Phase 1 corresponds to the design of firmware, software and hardware; it covers both TEE and additional software components;
- [T-Head] Phase 2 corresponds to the overall design of the hardware platform supporting the TEE;
- [T-Head] Phase 3 corresponds to the chipset and other hardware components manufacturing. The root key and material use to generate TEE identifier are set in this phase;
- [T-Head] Phase 4 covers software preparation (linking the TEE software and other software);
- [T-Head] Phase 5 consists of device assembling; it includes any initialization and configuration step necessary to bring the device to a secure device prior delivery to the end-user. The Trusted ROM is formatted in this phase;
- Phase 6 stands for the end-usage of the device.

The TOE operational phase starts in Phase 5.

2.5 Security functionality

The security functionality of the TOE in the scope of the evaluation (in the end-user phase) consists of:

- TEE instantiation through a secure initialization process using assets bound to the SoC, that ensures the authenticity and contributes to the integrity of the TEE code running in the device;
- Isolation of the TEE services, the TEE resources involved and all the TAs from the REE;
- Isolation between TAs and isolation of the TEE from the TAs;
- Protected communication interface between Client Applications (CAs) in the REE and TAs in the TEE;
- Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE;
- Random Number Generator (TRNG and DRBG which uses the NIST SP800-90A approved algorithm for generating the random numbers based on the seed);
- Cryptographic API for TAs (see Table 2-5);
- TA instantiation that ensures the authenticity and contributes to the integrity of the TA code;
- Monotonic TA instance time;
- Correct execution of TA services;
- TEE firmware integrity verification;
- Prevention of downgrade of TEE firmware;
- Debug mode not activated on production devices;
- Closed communication ports (e.g. Serial).

The TOE relies on the following internal cryptographic functionality:

- RSASSA PKCS1_V1_5_SHA256 (with 2048 bits key length) signature verification of TEE firmware upon initialization, based on hardware root of trust;

- RSASSA PKCS1_V1_5_SHA256 (with 2048 bits key length) signature verification of TA code upon application instantiation (loading), based on OEM certificate;
- AES-GCM 128 encryption/decryption of stored TA data, based on hardware root-of-trust for Trusted Storage, diversified per TA combined with HMAC_SHA256.

Note: GlobalPlatform recommendations for the TEE internal cryptographic functionality defined in [CRYPTO] include the deprecation of RSA with 2048 bit-long keys from January 1, 2024. However, this deprecation does not result of an actual known vulnerability as of this certification report's publication. The recommendation R.RSA_2048 for users of the certified Product addresses this non-conformity:

> **R.RSA_2048**
>
> Users of the certified Product shall ensure that the cryptographic algorithm RSA with 2048-bit keys is suitable for the TEE initialization and the TA signature verification in the contexts of use of the Product and shall take any appropriate measure otherwise.

Table 2-5 presents the cryptographic operations supported by the Product according with the [ST]. However, only those identified in FCS_COP.1 (cf. [ST]) are in the scope of the evaluation.

Table 2-5: List of cryptographic algorithms

Category	Algorithm identifier	Key length (bits)
AES	AES_ECB_NOPAD, AES_CBC_NOPAD, AES_CTR, AES_CCM, AES_GCM, AES_CCM	128, 192, 256
RSA Sign/Verify	RSASSA_PKCS1_V1_5_SHA1, RSASSA_PKCS1_V1_5_SHA256, RSASSA_PKCS1_V1_5_SHA512, RSASSA_PKCS1_PSS_MGF1_SHA1, RSASSA_PKCS1_PSS_MGF1_SHA256, RSASSA_PKCS1_PSS_MGF1_SHA512	2048, 4096
RSA Encryption	RSAES_PKCS1_V1_5, RSAES_PKCS1_OAEP_MGF1_SHA1, RSAES_PKCS1_OAEP_MGF1_SHA256, RSAES_PKCS1_OAEP_MGF1_SHA512, RSA_NOPAD	2048,4096
Hash	SHA2_256, SHA2_384, SHA2_512, SHA3_256, SHA3_384, SHA3_512	-
HMAC	HMAC_SHA2_256, HMAC_SHA2_512	64 bits for SHA2_256, 128 bits for SHA2_512
ECDSA	ECDSA	256
ECDH	ECDH_DERIVE_SHARED_SECRET	256

The TOE provides the following cryptographic operations to the TAs through the proprietary legacy API:

Category	Algorithm identifier	Key length (bits)
AES	AES_CBC_NOPAD, AES_CTR, AES_CCM, AES_GCM, AES_CCM	128, 192, 256

Category	Algorithm identifier	Key length (bits)
RSA Sign/Verify	RSASSA_PKCS1_V1_5_SHA1, RSASSA_PKCS1_V1_5_SHA256, RSASSA_PKCS1_V1_5_SHA512, RSASSA_PKCS1_PSS_MGF1_SHA1, RSASSA_PKCS1_PSS_MGF1_SHA256, RSASSA_PKCS1_PSS_MGF1_SHA512	2048, 4096
RSA Encryption	RSAES_PKCS1_V1_5, RSAES_PKCS1_OAEP_MGF1_SHA1, RSAES_PKCS1_OAEP_MGF1_SHA256, RSAES_PKCS1_OAEP_MGF1_SHA512, RSA_NOPAD	2048,4096
Hash	SHA2_256, SHA2_384, SHA2_512, SHA3_256, SHA3_384, SHA3_512	-
HMAC	HMAC_SHA2_256, HMAC_SHA2_512	64 bits for SHA2_256, 128 bits for SHA2_512
ECDSA	ECDSA	256
ECDH	ECDH_DERIVE_SHARED_SECRET	256

The recommendation R.CRYPTO_ALG for TA developers applies:

R.CRYPTO_ALG

Although the following algorithms are implemented in the Product, these are not in the scope of the evaluation and their usage is not recommended:

- RSASSA_PKCS1_V1_5_SHA1;
- RSASSA_PKCS1_PSS_MGF1_SHA1;
- RSAES_PKCS1_OAEP_MGF1_SHA1.

2.6 Objectives for the TOE environment

The security target of [ST] establishes the following objectives for the TOE environment, compliant with the TEE PP v1.3:

OE.INTEGRATION_CONFIGURATION: Integration and configuration of the TEE by the device manufacturer shall comply with the security guidelines defined by the TEE provider, which must include all recommendations issued from the TEE evaluation.

OE.PROTECTION_AFTER_DELIVERY: The TEE and its assets shall be protected after delivery and before entering the end-usage phase. The personnel using the TEE in the operational environment shall have the required skills to understand and apply the security guidelines.

OE.SECRETS: Management of secret data (e.g. generation, storage, distribution, destruction, loading into the product of cryptographic private keys, symmetric keys, user authentication data) performed outside the TEE shall enforce integrity and confidentiality of these data.

OE.TA_DEVELOPMENT: TA developers shall comply with the TA development guidelines set by the TEE provider. In particular, TA developers shall apply the following security recommendations during the development of the Trusted Applications:

- CA identifiers are generated and managed by the REE, outside the scope of the TEE; TAs do not assume that CA identifiers are genuine;

- TAs do not disclose any sensitive data to the REE through any CA (interaction with the CA may require authentication means);
- TAs shall not assume that data written to a shared buffer can be read unchanged later on; TAs should always read data only once from the shared buffer and then validate it;
- TAs should copy the contents of shared buffers into TA instance-owned memory whenever these contents are required to be constant.

OE.TA_MANAGEMENT: If the TEE allows managing the set of TAs, e.g. updating, replacing, deleting, and installing TAs, then a well-defined TA identification and TA signature policy shall ensure the authenticity of the application and prevent impersonation. That is, the entity responsible for TA identification and TA signature shall ensure that these operations are performed in a controlled environment through dedicated procedures, which prevent, by technical and/or organisational means from:

- Assigning the same identification to different applications;
- Signing applications that have not been identified following the applicable procedures;
- Unauthorized access to signature keys.

[INTEGR_GUIDE] addresses all the security objectives for the environment.

2.7 Clarification of the scope

The TOE does not comprise any pre-loaded TA.

The REE (including the TEE Client APIs) and the External DRAM hardware module are non-TOE components which are required for the operation of the TOE. These components are out of the scope of the evaluation.

There is only one configuration for the TOE.

The functional compliance of the TOE with GlobalPlatform API specification is not required by the TEE PP and is out of the scope of the evaluation.

T-Head development and manufacturing sites as well as the procedures applicable in Phases 1 to 5 are out of the scope of the evaluation.

3 Evaluation

3.1 Evaluation laboratory identification

The evaluation has been performed by DPLS Lab, located Room 701, building 7, No. 98, Lianshi Lake West Road, Mentougou District, Beijing, China 102308, accredited by GlobalPlatform under reference GP_AL_027.

3.2 Evaluated configuration

The evaluation addressed one TOE configuration, as defined in section 2.1. Any deviation from the indicated components brings the TOE outside the evaluated configuration.

The testing of the TOE has been performed on T-Head SoC embedding the *Xuantie TEE* components in Production mode.

3.3 Evaluation activities

The evaluation of the TOE has been performed on the basis of the following GlobalPlatform documentation:

- [TEE PP] TEE Protection Profile;
- [TEE EM] TEE Evaluation Methodology;
- [TEE AP] Application of Attack Potential to Trusted Execution Environment.

The evaluation activities consisted of:

- Vulnerability analysis of the TOE based on public sources and on developer's documentation including [ST], [INTEGR_GUIDE], [DEV_GUIDE] and [FINAL_GUIDE];
- Source code review of the TOE's software components;
- Testing of the GlobalPlatform TEE Internal Core API against the TEE Security Test Suite v1.0.1;
- Quality testing of random numbers generated by the TOE;
- Software and hardware-based TOE penetration testing.

The laboratory has also performed the following tasks:

- Conformity check of the security target [ST] against the TEE Protection Profile [TEE PP];
- Consistency check between the guidance documents [INTEGR_GUIDE], [DEV_GUIDE] and [FINAL_GUIDE], the objectives for the TOE operational environment in the [ST] and the result of the evaluation.

3.4 Evaluation results

The evaluation laboratory documented the evaluation activities and results in the following report:

- [ETR] *Xuantie TEE Detailed Technical Evaluation Report.*

The evaluation laboratory determined that:

- The security target [ST] is conformant to the TEE Protection Profile [TEE PP] (Core TEE PP without any PP-Modules);
- The TOE successfully passed the security functional testing and random numbers quality test;

- All the vulnerabilities identified during the source code review and testing campaigns have been corrected or discarded based on a specific analysis;
- The guidance [INTEGR_GUIDE] addresses the objectives for the TOE environment defined in the [ST] (see section 2.6);
- The TOE is resistant to attacks performed by an attacker possessing Enhanced-basic attack potential, as defined in [TEE PP] and [TEE AP], provided the objectives for the TOE operational environment hold and the guidance is applied.

The ETR does not provide any additional recommendation on the usage of the Product.

4 CERTIFICATION

4.1 Usage restrictions

The user of the certified Product must ensure that the following objectives, guidance and recommendations are applied:

- Objectives for the TOE operational environment (see section 2.6) defined in the security target [ST];
- Guidance [INTEGR_GUIDE], [DEV_GUIDE] and [FINAL_GUIDE];
- GlobalPlatform recommendations R.RSA_2048 and R.CRYPTO_ALG.

The security target, the guidance and this certification report should be distributed or made available to the users of the certified Product. Any other documentation delivered with the Product or made available to users is not included in the scope of the evaluation and therefore should not be relied upon when using the certified Product.

4.2 Conclusion

This certification report confirms that the evaluation of Xuantie TEE v1.0 has been performed as required by the GlobalPlatform Evaluation Methodology [TEE EM] and that there is sufficient evidence to affirm that the product meets the security functional requirements and AVA_VAN_AP.3 as defined in the security target [ST], provided the usage restrictions defined in section 4.1 are fulfilled.

Consequently, GlobalPlatform grants a Full Certificate to Xuantie TEE v1.0 in accordance with the TEE scheme Certification Process [TEE CP].

The user of the certified Product should consider the result of the certification within an appropriate risk management process and define the period after which the re-assessment of the Product is required.

Carolina Lavatelli
Scheme Owner

Guillaume Achten
c=US, st=California, l=Redwood
City,
serialNumber=AATL202309053
13272, o=GLOBALPLATFORM,
INC., cn=Guillaume Achten,
email=guillaume.achten@mello
nne.com
'00'02+ 09:44:57 2024.04.09

5 REFERENCES

Table 5-1: GlobalPlatform References

Document	Description	Ref.
GP_PRO_023	GlobalPlatform TEE Certification Process v2.0	[TEE CP]
GPD_SPE_021	GlobalPlatform Technology TEE Protection Profile v1.3	[TEE PP]
GPD_GUI_044	GlobalPlatform Technology TEE Evaluation Methodology v1.2	[TEE EM]
GPD_NOT_051	GlobalPlatform Technology Application of Attack Potential to Trusted Execution Environment v1.8.1 – Confidential	[TEE AP]
GP_TEN_053	GlobalPlatform Technology Cryptographic Algorithm Recommendations v2.0	[CRYPTO]
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 v1.1.2	[IAPI]

Table 5-2: Product References

Document	Description	Ref.
Security Target	Xuantie TEE Security Target v1.1.11, ref. STG90002	[ST]
Guidance	Guidance for SoC integrators v1.0, ref. STG90003	[INTEGR_GUIDE]
Guidance	Guidance for TA developers v1.0, ref. STG90004	[DEV_GUIDE]
Guidance	Guidance for TEE final users v1.0, ref. STG90005	[FINAL_GUIDE]
API	Xuantie C library APIs v1.0, ref. STG30004	[C API]
Evaluation Report	Xuantie TEE Detailed Technical Evaluation Report, version 3.1	[ETR]
NIST Special Publication	Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A Revision 1. June 2015	[NIST 800-90A]
FIPS Publication	FIPS 180-4 - Secure Hash Signature Standard (SHS), March 2012	[Hash]
FIPS Publication	FIPS 197 - Advanced Encryption Standard, November 2001	[AES]
IEEE Standard	IEEE Std 1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, April 2008	

Document	Description	Ref.
NIST Special Publication	NIST SP800-38A - Recommendation for Block Cipher Modes of Operation, October 2010	
RFC	RFC 1423 - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifier, February 1993s	
FIPS Publication	FIPS 46-3 - Data Encryption Standard (DES), October 1999	[3DES]
FIPS Publication	FIPS 81 - DES Mode of Operations	
RSA Laboratories Publication	PKCS#1 - RSA Cryptographic Standard. PCKS#1 v2.2. October 2012	[RSA]
FIPS Publication	FIPS 186-2 - Digital Signature Standard (DSS), January 2000	[DSA]
ANSI	ANSI X9.62 - Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECSDA)	
NIST Special Publication	NIST SP800-56A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007	[ECDH]
FIPS Publication	FIPS 186-4 - Digital Signature Standard (DSS), July 2013	
RSA Laboratories Publication	PKCS#3- Diffie-Hellman Key Agreement Standard	[DH]
RFC	RFC 4231 Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, December 2005	[HMAC]
RFC	RFC 2202 - Test cases for HMAC-MD5 and HMAC-SHA-1, September 1997	
NIST Special Publication	NIST SP800-38B - Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, May 2005	[CMAC]
RFC	RFC 3610 - Counter with CMC-MAC (CCM), September 2003	[AE]

6 Abbreviations

Table 6-1: Abbreviations

Term	Definition
AES	Advanced Encryption Standard
ATF	ARM Trusted Firmware
ARM	Advanced RISC (Reduced Instruction Set Computer) Machine
API	Application Programming Interface
CA	Client Application
DES	Data Encryption Standard
DH	Diffie-Hellman
DRAM	Dynamic RAM
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ETR	Evaluation Technical Report
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
HMAC	(keyed-)Hash Message Authentication Code
JTAG	Joint Test Action Group
MAC	Message Authentication Code
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
REE	Regular Execution Environment
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SHA	Secure Hash Algorithm
SoC	System-on-Chip
ST	Security Target
TA	Trusted Application
TEE	Trusted Execution Environment
TOE	Target of Evaluation
TRNG	True RNG