GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certificate of Security Evaluation

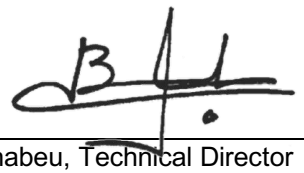
Alibaba Cloud Link TEE (Pro Edition) v1.1.3

Certification Number:	GP-TEE-2019/01
Issuance Date:	July 12th 2019
Sponsor:	Alibaba Cloud Computing Ltd.
Protection Profile:	TEE PP v1.2.1 – Base PP
PP-Modules:	☑ Time & Rollback v1.2.1 (Mode#1 and Mode#2) ☑ Debug v1.2.1 (Mode#2)
Certification Type:	☑ Full ☐ Restricted
Certification Report:	GP-TEE-2019/01-CR

Product Name:	Alibaba Cloud Link TEE (Pro Edition) v1.1.3
Configurations:	Mode#1 and Mode#2
Trusted OS / Developer:	TEE-Pro v1.1.3 / Alibaba Cloud Computing Ltd.
SoC / Developer:	i.MX6QuadPlus - MCIMX6QP6AVT1AB / NXP (China) Management Ltd.
Product Type:	☐ TEE on Final Device ☑ TEE on SoC ☐ TEE partial scope: ☐ HW/SW ☐ HW ☐ SW
Evaluation Type:	☑ Full ☐ Delta ☐ Fast-track
Security Evaluation Lab:	Beijing Zhihui Yunce Equipment Technology Co., Ltd (DPLS Lab)

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 laboratory evaluation. 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 Evaluation Secretariat Certification Report.

GlobalPlatform, Inc.



Gil Bernabeu, Technical Director

544 Hillside Road | Redwood City, CA 94062 | secretariat@globalplatform.org | www.globalplatform.

GLOBALPLATFORM® CERTIFIED TEE

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform TEE Security Evaluation Secretariat

Certification Report

GP-TEE-2019/01-CR v1.0

Issue date:	July 12th 2019
Product:	Alibaba Cloud Link TEE (Pro Edition) v1.1.3 Configurations: Mode#1 and Mode#2
Sponsor:	Alibaba Cloud Computing Ltd.
Developers:	Alibaba Cloud Computing Ltd. Building 8, NO.16, Zhuantang, Sci-tech Economic Block, Xihu District, Hangzhou, Zhejiang Province, China NXP (China) Management Ltd. 21F, BM InterContinental Business Center, 100 Yu Tong Road, Shanghai, China
Laboratory:	Beijing Zhihui Yunce Equipment Technology Co., Ltd (DPLS Lab) Room 701-3, Building 7, No. 98, Lianshihu Xilu, Mentougou District, Zip 102308, Beijing, China
Conformance:	TEE PP v1.2.1 – Base PP and PP-Modules: ☑ Time & Rollback (Mode#1 and Mode#2) ☑ Debug (Mode#2 only)
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 *Alibaba Cloud Link TEE (Pro Edition) v1.1.3, Configurations: Mode#1 and Mode#2*, developed by Alibaba Cloud Computing Ltd. and NXP (China) Management Ltd., registered under number GP180004.

The evaluation has been performed by accredited laboratory DPLS Lab in Beijing (China). The following documents constitute the basis for this evaluation: *Alibaba Cloud Link TEE-Pro V1.1.3, version 1.6, July 2019 [ST], NXP i.MX 6QuadPlus based SoC TEE-Pro Integration Guide, version 1.3, July 2019 [INTEGR_GUIDE] and Alibaba Cloud Link TEE-Pro Development Guide, version 1.3, July 2019 [DEV_GUIDE].*

The evaluation determined that the product, as identified in this report, meets GlobalPlatform's TEE security functional requirements at the assurance level AVA_TEE.2 and that the guidance includes all the necessary security recommendations to address the assumptions identified in the Security Target and the recommendations issued from the evaluation. The results of the evaluation are presented in the technical evaluation report *Alibaba-TEE GP180004 DTER V12, version 1.2, amended with Rollback annexes, version 1.0. [DTER].*

The certification determined that the evaluation has been performed in conformance with *GlobalPlatform TEE Protection Profile v1.2.1 [TEE PP]* with PP-Modules *Time&Rollback* in Mode#1 and Mode#2, and *Debug in* Mode#2, and *TEE Evaluation Methodology v1.0 [TEE EM]*. The certificate is valid provided all the usage restrictions defined in section 4.1 are fulfilled.

2 TEE Product

2.1 Identification

The TEE Product in this evaluation is Alibaba Cloud Link TEE (Pro Edition) v1.1.3 (TEE-Pro v1.1.3) developped by Alibaba Cloud Computing Ltd. and NXP (China) Management Ltd.:

Product Identification	
Product Name	Alibaba Cloud Link TEE (Pro Edition) v1.1.3 Configurations: Mode#1 and Mode#2
Developers	Alibaba Cloud Computing Ltd. (also referred as Alibaba) NXP (China) Management Ltd. (also referred as NXP)
Product Type	TEE on SoC

Two irreversible JTAG configurations for production Alibaba Cloud Link TEE (Pro Edition) v1.1.3 are considered:

- Mode#1: JTAG is permanently disabled;
- Mode#2: Secure JTAG is enabled upon e-fuse-password authentication.

These configurations are performed through e-fusing at device level. Open JTAG mode is not allowed.

The Target of Evaluation (TOE) consists of the set of components of the TEE Product that are listed in the following table, including the pre-loaded applications that contribute to the TOE's security functionality:

TOE Components Identification		**Developer**
SoC reference	NXP i.MX6QuadPlus - MCIMX6QP6AVT1AB	NXP (China) Management Ltd.
ROM code	NXP i.MX6QP ROM ARIK_N_02.01.00 Checksum (the last word of ROM space): 0x09CC079B	NXP (China) Management Ltd.
Pre-Loader boot code	NXP i.MX6QP uboot-imxrel_imx_4.9.88_2.0.0_ga	NXP (China) Management Ltd.
ATF	ATF release version 1.3.3 MD5: 541b976cecde7e9759a5bb001b6de745	Alibaba Cloud Computing Ltd.
TEE binary	Alibaba Cloud Link TEE (Pro Edition) version 1.1.3 MD5: 6c51118de92a5fe6db5aaa0f5ddd18b1 (includes the tstd and rpmb_mgrd system TAs)	Alibaba Cloud Computing Ltd.

Pre-loaded TAs	• tstd MD5: 3ad92293c5656650c9fc3b6797acd19a • rpmb_mgrd MD5: 615460e3e68073a313b3f782a352663d	Alibaba Cloud Computing Ltd.

The Rich OS (Linux 4.9.88), including the TEE client APIs, and the External DRAM hardware module are non-TOE components which are required for the operation of the TOE.

2.2 Documentation

The Security Target (ST) for this evaluation is:

- [ST] Alibaba Cloud Link TEE-Pro V1.1.3, version 1.6, July 2019

The ST is compliant with TEE Protection Profile v1.2.1 including the Base PP and the following PP-Modules:

- "Time & Rollback" in Mode#1 and Mode#2;
- "Debug" in Mode#2.

The guidance for device integrators and application developers consists of the following documents:

- [INTEGR_GUIDE] NXP i.MX 6QuadPlus based SoC TEE-Pro Integration Guide, version 1.3, July 2019;
- [DEV_GUIDE] Alibaba Cloud Link TEE-Pro Development Guide, version 1.3, July 2019.

2.3 Architecture

The hardware architecture of the TOE consists of i.MX6 Quad Plus, which is a 4-core ARM v7-A Cortex-A9 Processor with security extension, internal physical memories, a Memory Protection Unit, AES crypto accelerator, random number generator (TRNG for physical source and DRBG using NIST SP8000-90A approved algorithm) and peripherals connected through AXI-based Bus, some of which are accessible only from the Secure World through the Trusted OS, e.g. JTAG (in Mode#2).

An external persistent memory (e.g. eMMC) with RPMB partition is required for rollback protection.

Note: The external DRAM hardware module is not part of the SoC but external DRAM data is encrypted on the fly by the SoC cryptographic module (CAAM module).

The firmware/software architecture of the TOE consists of ROM boot code, Pre-loader, ATF, and Alibaba's Trusted OS TEE-Pro.

Note: The TOE does not include the Rich Execution Environment (REE) which consists essentially of Linux 4.9.88, the TEE client APIs and the applications running on top.

The TOE provides the following software interfaces:

- A proprietary communication interface with the REE;
- GlobalPlatform API (see below).

The TOE does not provide any additional Proprietary APIs to TAs.

The TOE implements the GlobalPlatform API listed below, for which Alibaba declares full functional compliance in the ST:

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	1.1
GPD_EPR_017	TEE Internal Core API Specification v1.0 Errata and Precisions	1.0
	TEE Internal Core API Specification v1.0 Errata and Precisions	3.0

2.4 Life-cycle

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

- [Alibaba] Phase 1 corresponds to the design of TEE firmware and software;
- [NXP] Phase 2 corresponds to the design of hardware and ROM code;
- [NXP] Phase 3 corresponds to the SoC manufacturing and e-Fusing (device root key);
- [Alibaba & NXP] Phase 4 corresponds to the integration, validation and preparation of the software to load in the product;
- [Alibaba] Phase 5 corresponds to the device manufacturing. In this phase, the TEE is initialized and personalized, before delivery;
- Phase 6 stands for the end-usage of the device.

The TOE operational phase starts in Phase 6.

2.5 Security Functionality

The security functionality of the TOE 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 Trusted Applications from the REE;
- Isolation between Trusted Applications and isolation of the TEE from Trusted Applications;
- Protected communication interface between CAs and TAs within the TEE, including communication endpoints in the TEE;
- Trusted storage of TA and TEE data and keys, ensuring consistency (at READ operation time), confidentiality, atomicity and binding to the TEE;
- Random Number Generator;
- Cryptographic API for TAs (see below);
- TA instantiation that ensures the authenticity and contributes to the integrity of the TA code;
- Monotonic TA instance time;
- Monotonic TA persistent time;
- Correct execution of TA services;
- TEE firmware integrity verification;
- Prevention of downgrade of TEE firmware;

- Prevention of downgrade of TA code and persistent data;
- Serial port disabled in all production TOEs;
- JTAG: two irreversible configurations for production TOE, performed through efusing at device level
  - Permanently disabled (Mode#1);
  - Secure (Mode#2): JTAG enabled upon efuse-password authentication.

The TOE relies on the following cryptographic functionality:

- RSASSA PKCS1_V1_5_SHA256 (with 4096 bits key length) signature verification of TEE firmware upon initialization, based on hardware root of trust;
- RSASSA PKCS1_V1_5_SHA256 (with 4096 bits key length) signature verification of TA code upon application instantiation (loading), based on OEM certificate;
- AES-CTR 256 encryption/decryption of stored TA data (meta data and stream data), AES_CTR 256 for objects sessions, based on hardware root-of-trust for Trusted Storage, diversified per TA combined with AES_ECB_NOPAD.

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

Category	**Algorithm identifier**	**Key length (bits)**
AES	TEE_ALG_AES_ECB_NOPAD, TEE_ALG_AES_CBC_NOPAD, TEE_ALG_AES_CTR, TEE_ALG_AES_CMAC, TEE_ALG_AES_CTS, TEE_ALG_AES_XTS, TEE_ALG_AES_CCM, TEE_ALG_AES_GCM, TEE_ALG_AES_CBC_MAC_NOPAD, TEE_ALG_AES_CBC_MAC_PKCS5	128, 192, 256
DES	TEE_ALG_DES_ECB_NOPAD, TEE_ALG_DES_CBC_NOPAD, TEE_ALG_DES_CBC_MAC_NOPAD, TEE_ALG_DES_CBC_MAC_PKCS5	64
DES3	TEE_ALG_DES3_ECB_NOPAD, TEE_ALG_DES3_CBC_NOPAD, TEE_ALG_DES3_CBC_MAC_NOPAD, TEE_ALG_DES3_CBC_MAC_PKCS5	112, 168
RSA Sign/Verify	TEE_ALG_RSASSA_PKCS1_V1_5_MD5, TEE_ALG_RSASSA_PKCS1_V1_5_SHA1, TEE_ALG_RSASSA_PKCS1_V1_5_SHA224, TEE_ALG_RSASSA_PKCS1_V1_5_SHA256, TEE_ALG_RSASSA_PKCS1_V1_5_SHA384, TEE_ALG_RSASSA_PKCS1_V1_5_SHA512, TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA1, TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA224, TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA256, TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA384, TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA512	up to 4096

Category	Algorithm identifier	Key length (bits)
RSA Encryption	TEE_ALG_RSAES_PKCS1_V1_5, TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA1, TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA224, TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA256, TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA384, TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA512, TEE_ALG_RSA_NOPAD	up to 4096
DH	TEE_ALG_DH_DERIVE_SHARED_SECRET	-
Hash	TEE_ALG_MD5, TEE_ALG_SHA1, TEE_ALG_SHA224, TEE_ALG_SHA256, TEE_ALG_SHA384, TEE_ALG_SHA512	-
HMAC	TEE_ALG_HMAC_MD5, TEE_ALG_HMAC_SHA1, TEE_ALG_HMAC_SHA224, TEE_ALG_HMAC_SHA256, TEE_ALG_HMAC_SHA512	-
DSA	TEE_ALG_DSA_SHA1, TEE_ALG_DSA_SHA224, TEE_ALG_DSA_SHA256	
ECDSA	TEE_ALG_ECDSA_P192, TEE_ALG_ECDSA_P224, TEE_ALG_ECDSA_P256, TEE_ALG_ECDSA_P384, TEE_ALG_ECDSA_P521	up to 521
ECDH	TEE_ALG_ECDH_P192, TEE_ALG_ECDH_P224, TEE_ALG_ECDH_P256, TEE_ALG_ECDH_P384, TEE_ALG_ECDH_P521	up to 521

The following recommendation for TA developers applies:

R.CRYPTO_ALG

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

Not recommended algorithms
TEE_ALG_AES_CTS, TEE_ALG_AES_XTS, TEE_ALG_AES_CCM, TEE_ALG_AES_GCM, TEE_ALG_AES_CBC_MAC_NOPAD, TEE_ALG_AES_CBC_MAC_PKCS5
TEE_ALG_DES_ECB_NOPAD, TEE_ALG_DES_CBC_NOPAD, TEE_ALG_DES_CBC_MAC_NOPAD, TEE_ALG_DES_CBC_MAC_PKCS5
TEE_ALG_DES3_ECB_NOPAD, TEE_ALG_DES3_CBC_NOPAD, TEE_ALG_DES3_CBC_MAC_NOPAD, TEE_ALG_DES3_CBC_MAC_PKCS5
TEE_ALG_DH_DERIVE_SHARED_SECRET
TEE_ALG_DSA_SHA1, TEE_ALG_DSA_SHA224, TEE_ALG_DSA_SHA256
TEE_ALG_ECDSA_P192, TEE_ALG_ECDSA_P224, TEE_ALG_ECDSA_P256, TEE_ALG_ECDSA_P384, TEE_ALG_ECDSA_P521
TEE_ALG_ECDH_P192, TEE_ALG_ECDH_P224, TEE_ALG_ECDH_P256, TEE_ALG_ECDH_P384, TEE_ALG_ECDH_P521

2.6 Assumptions

The Security Target of Alibaba Cloud Link TEE (Pro Edition) v1.1.3 establishes the following assumptions:

- A.PROTECTION_AFTER_DELIVERY, A.JTAG_PASSWORD_GENERATION (applicable to configuration Mode#2) and A.SERIAL_DEBUG that apply to the integration phase;

- A.TA_DEVELOPMENT, A.EFFECTIVE_WRITE, A.TA_MANAGEMENT and A.UUID_MANAGEMENT that apply to the TA developers.

The integration guide [INTEGR_GUIDE] and the developer guide [DEV_GUIDE] address all the assumptions.

The text of the assumptions is the following:

A.PROTECTION_AFTER_DELIVERY (from TEE PP)

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

A.TA_DEVELOPMENT (from TEE PP)

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

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

A.EFFECTIVE_WRITE

During a decision process within a single power cycle and before validating the decision, the TA developer is assumed to ensure that all the WRITE operations of persistent values are effective, by confirming these values through corresponding READ operations.

Application note:

The decision process can be, for instance, a financial or a DRM transaction.

The READ operation is necessary because consistency is ensured upon READ (not WRITE).

This is a refinement of A.TA_DEVELOPMENT.

A.TA_MANAGEMENT

TA developers carefully consider the following TEE principles with regard to TA and Trusted Storage management during the development of their applications:

- The TA identification (or TA identity) is composed of a TA UUID and is managed by the entity in charge of signing the application;
- The TEE does not provide TA install/uninstall functions;
- TA loading and TA session opening are performed at the same time upon successful verification of the TA code signature, provided no “single-instance” application with the same TA identification is already running;
- Multiple application versions with the same TA identity may run concurrently and access the same

set of data provided the TA is “multi-instance”;
- The ownership of persistent data stored in a Trusted Storage object associated with a given TA identity is automatically granted to any application instance that is loaded with such TA identity;
- Trusted Storage objects are never erased by the TEE (no TA install/uninstall functionality provided) and then remain accessible without any limitation of time or kind of operation (e.g. creation, read, write, delete).

Consequently, TA developers are assumed to internalize the management of TA and TA persistent data life cycle within the TA itself.

Application note:

This is a refinement of A.TA_DEVELOPMENT.

A.UUID_MANAGEMENT

The entity responsible for TA identification and TA signature ensures that these operations are performed in a controlled environment through dedicated procedures, which prevent, by technical and/or organizational means from:
- Assigning the same identification to different applications;
- Signing applications that have not been identified following the applicable procedures;
- Accessing to TA signature keys without authorization.

A.JTAG_PASSWORD_GENERATION (applicable to configuration Mode#2)

It is assumed that each device is assigned a unique JTAG password.

The entity responsible for JTAG password generation ensures that these operations are performed in a controlled environment through dedicated procedures, which prevent, by technical and/or organizational means from:

- Assigning the same password to different SoC;
- Assigning predictable password to SoC, even based on a cryptographic derivation

A.SERIAL_DEBUG

It is assumed that serial port is disabled in all production TOEs.

2.7 Clarification of Scope

The External DRAM hardware module is a non-TOE component, which is out of the evaluation scope.

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.

Alibaba Cloud Computing Ltd. and NXP (China) Management Ltd. development and manufacturing sites as well as the procedures applicable in Phases 1 to 5 are out of the scope of the evaluation.

Both TOE configurations Mode#1 and Mode#2 provide full rollback protection of TA code and data, through the use of RPMB partition.

Authentication-based debug through the JTAG port is allowed only in configuration Mode#2. In Mode#1, the JTAG port is disabled. The serial port is disabled in all configurations.

3 Evaluation

3.1 Evaluation Laboratory Identification

The TOE has been evaluated by DPLS Lab, located Room 701-3, Building 7, No. 98, Lianshihu Xilu, Mentougou District, Zip 102308, Beijing, China.

3.2 Evaluated Configuration

The evaluation addressed two TEE Product configurations, as defined in section 2.1. Note that any deviation from the indicated components versions brings the TOE outside the evaluated configurations.

The testing of the TOE has been performed on NXP devices embedding the Alibaba Cloud Link TEE (Pro Edition) v1.1.3 components, in three operation modes:

- Development mode, with activated debug features and root privilege;
- Production mode
  - Configuration Mode#1: JTAG disabled;
  - Configuration Mode#2: Authentication-based JTAG enabled.

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 CAT] TEE Common Automated Tests;
- [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] and [DEV_GUIDE];
- Source code review of the TOE's software components;
- Testing of the GlobalPlatform TEE Internal Core API against the TEE Security Test Suite v1.0.2;
- 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] and [DEV_GUIDE], the assumptions in the [ST] and the recommendations issued from the evaluation.

3.4 Evaluation Results

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

- [DTER] Alibaba-TEE GP180004 DTER V12, amended with Rollback annexes, version 1.0.

The evaluation laboratory raised one security recommendation that introduces some limitations on the usage of the TOE, which are included in the [ST] and in the [DEV_GUIDE], namely:

- **R.CRYPTO_ALG,** which lists the cryptographic APIs that should not be used.

The evaluation laboratory determined that:

- The Security Target [ST] is conformant to the TEE PP v1.2.1 - Base PP with PP-Modules:
  - "Time & Rollback" in Mode#1 and Mode #2;
  - "Debug" in Mode#2 (secure JTAG);
- 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 have given rise to security usage recommendations;
- The Security Target [ST] and the guidance [INTEGR_GUIDE] and [DEV_GUIDE] address all the assumptions listed in section 2.6 and all the security recommendations;
- The TOE is resistant to attacks performed by an attacker possessing TEE-Low attack potential, as defined in [TEE PP] and [TEE AP], provided the assumptions hold and the recommendations are applied.

4 Certification

4.1 Usage Restrictions

The user of the certified product must ensure that all the assumptions and security recommendations stipulated in the [ST] and the guidance [INTEGR_GUIDE], [DEV_GUIDE] are fulfilled. This includes:

- A.PROTECTION_AFTER_DELIVERY, A.JTAG_PASSWORD_GENERATION (applicable to configuration Mode#2 only), A.SERIAL_DEBUG , A.TA_DEVELOPMENT, A.EFFECTIVE_WRITE, A.TA_MANAGEMENT and A.UUID_MANAGEMENT (see section 2.6);
- R.CRYPTO_ALG (see section 2.5).

The Security Target and the guidance 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 Alibaba Cloud Link TEE (Pro Edition) v1.1.3 has been performed as required by the GlobalPlatform TEE Evaluation Methodology [TEE EM] and that there is sufficient evidence to affirm that the product meets its Security Target [ST] and the requirements of AVA_TEE.2, provided all the usage restrictions defined in section 4.1 are fulfilled. Consequently, GlobalPlatform issues the Full Certificate for Alibaba Cloud Link TEE (Pro Edition) v1.1.3 in conformity with the scheme Certification Process [TEE CP][TEE CP].

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

5 References

Table 5-1: GlobalPlatform References

Document	Description	Ref
GP_PRO_023	GlobalPlatform TEE Certification Process v1.0	[TEE CP]
GPD_SPE_021	GlobalPlatform TEE Protection Profile v1.2.1	[TEE PP]
GPD_GUI_044	GlobalPlatform TEE Evaluation Methodology v1.0	[TEE EM]
GPD_NOT_051	GlobalPlatform Application of Attack Potential to Trusted Execution Environment v1.5.0.3 – Confidential	[TEE AP]
GPD_SPE_050	GlobalPlatform TEE Common Automated Tests v1.0 As amended by GlobalPlatform TEE Security Test Suite v1.0.2	[TEE CAT]
GPD_SPE_007	GlobalPlatform TEE Client API Specification v1.0	
GPD_EPR_028	GlobalPlatform TEE Client API Specification v1.0 Errata and Precisions v2.0	
GPD_SPE_010	GlobalPlatform TEE Internal Core API Specification v1.1	
GPD_EPR_017	GlobalPlatform TEE Internal Core API Specification v1.0 Errata and Precisions v1.0	
	GlobalPlatform TEE Internal Core API Specification v1.0 Errata and Precisions v3.0	

Table 5-2: Product References

Document	Description	Ref
Security Target	Alibaba Cloud Link TEE-Pro V1.1.3, version 1.4, July 2019 (version used for the evaluation) SHA256(ALICLD_TEE_PRO_ST_201905.pdf)=d2b3e30928e96453bbf1f43ea665531abd886e8949f43e8b90b90703cd3e0bfd Alibaba Cloud Link TEE-Pro V1.1.3, version 1.6, July 2019 (editorial update requested for certification) SHA256(ALICLD_TEE_PRO_ST_201907.pdf)=c8561558bbadfa754d27828571242eff4c950827a4f3ea19d9177fb9ed0a3e22	[ST]

Document	Description	Ref
Guidance	NXP i.MX 6QuadPlus based SoC TEE-Pro Integration Guide, version 1.2, May 2019 (version used for the evaluation) SHA256(NXP i.MX 6QuadPlus based SoC TEE-Pro Integration Guide.pdf)=696c56a46af11bd62ec075c39a3b64b5fb86cc5ec17d690b813788054779e6da NXP i.MX 6QuadPlus based SoC TEE-Pro Integration Guide, version 1.3, July 2019 (editorial update requested for certification) SHA256(Alibaba Cloud Link TEE-Pro Development Guide.pdf)=36a73f8ac88b15f634ebe226dbae1638c9438d998bef498bf38ca712e6ce0ab2	[INTEGR_GUIDE]
Guidance	Alibaba Cloud Link TEE-Pro Development Guide, version 1.2, May 2019 (version used for the evaluation) SHA256(Alibaba Cloud Link TEE-Pro Development Guide.pdf)=1b3f9c786f5dffb4f1a77fb2556ddb91b3fc5c6e9fe98ce7fc9cd382c18b6d52 Alibaba Cloud Link TEE-Pro Development Guide, version 1.3, July 2019 (editorial update requested for certification) SHA256(NXP i.MX 6QuadPlus based SoC TEE-Pro Integration Guide.pdf)=9ad44fb113893bc3c3bbe81f9fcacdb4b7c0edcd641043d10a451b15785a7a78	[DEV_GUIDE]
Evaluation Report	Alibaba-TEE GP180004 DTER V12, version 1.2, amended with Rollback annexes, version 1.0 SHA256(Alibaba-TEE GP180004 DTER V12) = 4f9bcbac44e508f2bfe04c8a73af4c5112de9e027b927e09f9cc46a8b8af5dbf SHA256(Alibaba-TEE GP180004 DTER V12 Annex-rollback.pdf)= 958fe4a51175583498fa3f3a9fab6b97c4028640aacd4b081447551e26e52791 SHA256(anti-rollback.pdf)= c2df2c9fc2202cadacf3c3804adb66569e0b7e5f08f76a27d84c364c4ac78767 SHA256(rollback_questions-dpls.pdf)= 318759cf4a7aa80a946b279d41e2bd0235d66ce929894598feab040f2aa49511	[DTER]

Document	Description	Ref
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	
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]
Publication	FIPS 186-4 - Digital Signature Standard (DSS), July 2013	[ECDSA]
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]
NIST Special Publication	NIST SP800-38D - Recommendation for Block Cipher Modes of Operation: Galois/CounterMode (GCM) and GMAC, November 2007	

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
DTER	Detailed Technical Evaluation 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	Rich 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

Mounji Methlouthi

Signature numérique de Mounji Methlouthi
DN : c=US, cn=Mounji Methlouthi, email=mounji.methlouthi@smart-consulting.com
Date : 2019.07.17 18:08:17 +02'00'