GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certificate of Security Evaluation

Kinibi 410A

Certification Number:	GP-TEE-2019/03
Issuance Date:	December 3rd 2019
Sponsor:	Trustonic
PP-Conformance:	None
Certification Type:	☑ Full ☐ Restricted
Certification Report:	GP-TEE-2019/03-CR

Product Name:	Kinibi 410A
Configurations:	Normal mode and RP_SFS mode
Trusted OS / Developer:	Trustonic
SoC / Developer:	NA
Product Type:	☐ TEE on Final Device ☐ TEE on SoC ☑ TEE partial scope: ☐ HW ☐ FW ☑ SW
Evaluation Type:	☑ Full ☐ Delta ☐ Fast-track
Security Evaluation Lab:	Riscure B.V.

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

GLOBALPLATFORM® CERTIFIED TEE

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform TEE Security Evaluation Secretariat

Certification Report

GP-TEE-2019/03-CR v1.0

Issue date:	2019.12.03
Product:	Kinibi 410A Configurations: Normal mode and RP_SFS mode
Sponsor:	Trustonic 10 Station Road, Cambridge CB1 2JD (UK)
Developer:	Trustonic 10 Station Road, Cambridge CB1 2JD (UK)
Laboratory:	Riscure B.V. Delftechpark 49, 2628 XJ Delft, The Netherlands
PP-Conformance:	No conformance claims
Product Type:	☐ TEE on Final Device ☐ TEE on SoC ☑ TEE partial scope: ☐ HW ☐ FW ☑ 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

1 Executive Summary 4

2 Product 5
2.1 Identification 5
2.2 Documentation 5
2.3 Architecture 6
2.4 Life-cycle 6
2.5 Security Functionality 7
2.6 Security Objectives for the Operational Environment 10
2.7 Clarification of Scope 13

3 Evaluation 14
3.1 Evaluation Laboratory Identification 14
3.2 Evaluated Configuration 14
3.3 Evaluation Activities 14
3.4 Evaluation Results 14

4 Certification 16
4.1 Usage Restrictions 16
4.2 Conclusion 16

5 References 17

6 Abbreviations 20

Tables

Table 5-1: GlobalPlatform References 17

Table 5-2: Product-related References and Standards 17

Table 6-1: Abbreviations 20

1 Executive Summary

This document constitutes the Certification Report for the evaluation of Kinibi 410A, Configurations: Normal mode and RP_SFS mode, source code revision 90532, developed by Trustonic, registered under number GP190005. Kinibi 410A is a Trusted OS for Arm TrustZone-based Trusted Execution Environment (TEE).

The evaluation has been performed by accredited laboratory Riscure B.V. in Delft (The Netherlands). The following documents constitute the basis for this evaluation: *Kinibi 410A Security Target, version 1.5, August 2019 [ST]*, and guidance *Kinibi Integration Manual (July 15, 2019) [Integr_guide]*, *Kinibi Developer's Guide v5.2 [Dev_guide]*, *Kinibi API Documentation API Level 11 (July 16, 2019), Kinibi Driver Developer's Guide v2.8 and Kinibi Driver API Documentation v2.12 [API&Driver_guide]*, *Kinibi v410A Operational User Guidance v1.4 [OP_User_guide], Kinibi v410A Preparative Procedures Guidance v1.4 [Prep_Procedures] and ALC_DEL - Kinibi Delivery v1.2 [Delivery_Guide].*

The evaluation determined that the product, as identified in this report, meets the security functional requirements stated in *Kinibi 410A Security Target, version 1.5, August 2019 [ST]* at the assurance level AVA_TEE.2 for software attacks, and that the guidance provides security recommendations to address the objectives for the TOE environment that are defined in the Security Target and the recommendations issued from the evaluation. The results of the evaluation are presented in the technical evaluation report *Kinibi v4.10A – Security Evaluation Report, version 1.5 [DTER].* Hardware and hardware-based software attacks are out of the scope.

The certification determined that the evaluation was performed in conformance with *TEE Evaluation Methodology v1.0.0.2 [TEE EM]* for the evaluation of software TEE-parts (Trusted OS) by source code inspection. The certificate is valid provided all the usage restrictions defined in section 4.1 are fulfilled.

2 Product

2.1 Identification

The Product in this evaluation is Trusted OS Kinibi 410A, developped by Trustonic:

Product Identification	
Name	Kinibi 410A Configurations: Normal mode and RP_SFS mode
Developer	Trustonic
Type	TEE-Part (TEE Trusted OS)

Two configurations are possible:

- Normal mode: Secure Storage is not rollback-protected.
- RP_SFS mode: Secure Storage rollback protection is enforced with RPMB support.

The Target of Evaluation (TOE) consists of the source code[1] listed in the following table:

TOE Components Identification		**Developer**
Kinibi 410A source code	Kinibi 410A V003-r1 (revision 90532) Package: Kinibi-Src-410A-V003-r1-20190109.143150-1-20190109_143013_36.zip SHA256: cc598c4ba700d338a5798f71d122593d6d344de367c654f388a80a4429bae854	Trustonic

The following TAs are included in the image of the TOE:

Pre-installed TAs		Developer
TAs included in the image	DrSFS v410a-v003 DrCrypto v410-v003	Trustonic

2.2 Documentation

The Security Target (ST) for this evaluation is:

- [ST] Kinibi 410A Security Target, version 1.5, August 2019

The ST does not claim conformance with any PP. However, the ST is based on and consistent with:

- TEE Protection Profile v1.2.1
- Time & Rollback v1.2.1 (in RP_SFS mode)

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

[1] The TOE's binary reference is not provided here since this is a source-code-based evaluation.

- [Integr_guide] Kinibi Integration Manual (July 15, 2019)
- [Dev_guide] Kinibi Developer's Guide v5.2
- [API&Driver_guide] Kinibi API Documentation API Level 11 (July 16, 2019), Kinibi Driver Developer's Guide v2.8 and Kinibi Driver API Documentation v2.12
- [OP_User_guide] Kinibi v410A Operational User Guidance v1.4, 2019
- [Prep_Procedures] Kinibi v410A Preparative Procedures Guidance v1.4, 2019
- [Delivery_Guide] ALC_DEL - Kinibi Delivery v1.2, 2019.

2.3 Architecture

The TOE (Kinibi 410A) consists of the following software components, expected to run in the Secure World of an Arm-TrustZone SoC: MTK (microkernel), RTM (memory and session management, task loading, message passing and exception handling), McLib (library for TAs and Trusted Drivers, includes GlobalPlatform TEE Internal API and proprietary APIs), CR (crypto driver), STH2 (storage driver) and SPT2 (Secure Storage Proxy). The RPMB driver that is required in RP_SFS mode is not part of the TOE.

The TOE provides the following software interfaces:

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

The TOE implements the following GlobalPlatform APIs, for which Trustonic has declared full functional compliance in the Security Target.

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	1.1.1

The TOE also provides the following Proprietary APIs, developed by Trustonic:

Reference	Developer	Version	Content
[TR-DEVAPI]	Trustonic	410A	API level 11 for TAs
[TR-DRVAPI]	Trustonic	410A	API restricted to Trusted OS Drivers

2.4 Life-cycle

The TOE life cycle is split in 4 development and manufacturing phases and a final end-user phase:

- Phase 1 corresponds to Kinibi 410A design and development
- Phase 2 corresponds to Kinibi 410A porting for a specific Silicon Provider SoC
- Phase 3 corresponds to SIP and OEM integration, validation and preparation of the software to load in the product that will include the SoC secure firmware, the Kinibi 410A, any pre- installed Trusted Application and Trusted Drivers, and additional software required to use the product (e.g. REE, Client Applications)

- Phase 4 corresponds to Kinibi 410A flashing on the hardware, root-of-trust injection and device assembling (it includes the initialization and configuration steps necessary to bring the device to a secure state prior delivery to the end-user)
- Phase 5 stands for the end-usage of the device.

The delivery of Kinibi 410A occurs at the end of Phase 2. The TOE operational phase starts in Phase 3.

2.5 Security Functionality

The security functionality of the TOE in the end-user phase consists of:

- TOE components authenticity and rollback protection
- Memory management
- Isolation of Kinibi 410A, TAs and Trusted Drivers from the REE
- Isolation between TAs and isolation of the Kinibi 410A and its Trusted Drivers from TAs
- Identification of applications
- Protected communication interface between Client Applications (CAs) in the REE and TAs in the TEE
- Trusted storage of TA and Kinibi 410A data and keys, ensuring consistency, confidentiality, atomicity and device binding
- Cryptographic APIs for TAs (see below)
- Random Number Generator (DRBG NIST SP 800-90A Hash- DRBG with SHA256 algorithm, seeded by the underlying platform)
- Function to retrieve the device identification
- Instantiation of TAs ensuring authenticity (contributes to the integrity of the Trusted Drivers and TA code
- Monotonic TA instance time
- Correct execution of TA services.

The TOE relies on the following cryptographic functionality:

- For the authenticity of the Trusted Drivers and TA code:
  - RSA_SHA256_PSS with key size >= 2048
  - HMAC-SHA256 with key size 256
  - AES-128 CBC
  - SHA-256 truncated to 128 bits
- For the consistency and the confidentiality of the Trusted Storage:
  - HMAC-SHA256 with key size 256
  - AES-128 CBC
  - SHA-256 truncated to 128 bits.

In RP_SFS mode, the TOE provides the following functionality as per Time & Rollback PP-Module:

- Monotonic TA persistent time

- Integrity of TA code and persistent data
- Prevention of downgrade of TA code and persistent data.

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

Category	**Algorithm identifier (GP API)**	**Key length (bits)**
AES	AES_ECB_NOPAD AES_CBC_NOPAD AES_CTR AES_CTS AES_XTS AES_CCM AES_GCM AES_CBC_MAC_NOPAD, AES_CBC_MAC_PKCS5 AES_CMAC	128, 192, 256
DES3	DES3_ECB_NOPAD DES3_CBC_NOPAD DES3_CBC_MAC_NOPAD DES3_CBC_MAC_PKCS5	112, 168
RSA Sign/Verify	RSASSA_PKCS1_V1_5_SHA224 RSASSA_PKCS1_V1_5_SHA256 RSASSA_PKCS1_V1_5_SHA384 RSASSA_PKCS1_V1_5_SHA512 RSASSA_PKCS1_PSS_MGF1_SHA224 RSASSA_PKCS1_PSS_MGF1_SHA256 RSASSA_PKCS1_PSS_MGF1_SHA384 RSASSA_PKCS1_PSS_MGF1_SHA512	Between 256 and 4096 bits, multiple of 64 bits.
RSA Encryption	RSAES_PKCS1_OAEP_MGF1_SHA224 RSAES_PKCS1_OAEP_MGF1_SHA256 RSAES_PKCS1_OAEP_MGF1_SHA384 RSAES_PKCS1_OAEP_MGF1_SHA512 RSA_NOPAD	Between 256 and 4096 bits, multiple of 64 bits.
DSA	DSA_SHA224	DSA_SHA224: pbits = 2048, qbits = 224
	DSA_SHA256	DSA_SHA256: pbits = 3072, qbits = 256512 <= pbits <= 3072

Category	Algorithm identifier (GP API)	Key length (bits)
		and 160 <= qbits <= 256 (in steps of 8 bits), regardless of hash function.
DH	DH_DERIVE_SHARED_SECRET	Between 256 and 2048 bits, multiple of 8 bits.
Hash	SHA224, SHA256, SHA384, SHA512	-
HMAC	HMAC_SHA224, HMAC_SHA256, HMAC_SHA384, HMAC_SHA512	-
ECDSA	ECDSA	P192, P224, P256, P384, P521
ECDH	ECDH	P192, P224, P256, P384, P521

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

Category	Algorithm identifier (Legacy API)	Key length (bits)
AES	AES_128_CBC_NOPAD, AES_128_CBC_ISO9797_M1, AES_128_CBC_ISO9797_M2 AES_128_CBC_PKCS5, AES_128_CBC_PKCS7, AES_128_ECB_NOPAD, AES_128_CTR_NOPAD, AES_128_ECB_ISO9797_M1, AES_128_ECB_ISO9797_M2, AES_128_ECB_PKCS5, AES_128_ECB_PKCS7 AES_256_CBC_NOPAD, AES_256_CBC_ISO9797_M1, AES_256_CBC_ISO9797_M2, AES_256_CBC_PKCS5, AES_256_CBC_PKCS7, AES_256_ECB_NOPAD, AES_256_CTR_NOPAD, AES_256_ECB_ISO9797_M1, AES_256_ECB_ISO9797_M2, AES_256_ECB_PKCS5, AES_256_ECB_PKCS7	128, 256
DES3	3DES_2KEY_CBC_ISO9797_M1, 3DES_2KEY_CBC_ISO9797_M2 3DES_2KEY_CBC_NOPAD, 3DES_2KEY_CBC_PKCS5 3DES_3KEY_CBC_ISO9797_M1, 3DES_3KEY_CBC_ISO9797_M2 3DES_3KEY_CBC_NOPAD, 3DES_3KEY_CBC_ PKCS5	112, 168
RSA Sign/Verify	RSA_SHA_PKCS1, RSA_SHA224_PKCS1, RSA_SHA256_PKCS1, RSA_SHA384_PKCS1, RSA_SHA512_PKCS1, RSA_SHA224_PSS, RSA_SHA256_PSS, RSA_SHA384_PSS, RSA_SHA512_PSS	Between 256 and 4096 bits, multiple of 64 bits.
RSA Encryption	RSA_ISO14888, RSA_NOPAD, RSA_PKCS1, RSA_SHA224_OAEP, RSA_SHA256_OAEP RSA_SHA384_OAEP, RSA_SHA512_OAEP, RSACRT_SHA224_OAEP, RSACRT_SHA256_OAEP, RSACRT_SHA384_OAEP, RSACRT_SHA512_OAEP	Between 256 and 4096 bits, multiple of 64 bits.
DSA	DSA_RAW, DSA_HASHED	up to 3072
DH	DH_KEYPAIR	Between 256 and 2048 bits, multiple of 8 bits.
Hash	SHA224, SHA256, SHA384, SHA512	-
HMAC	HMAC_SHA224, HMAC_SHA_256, HMAC_SHA384, HMAC_SHA512	-

Category	Algorithm identifier (Legacy API)	Key length (bits)
ECDSA	ECDSA_RAW, ECDSA_HASHED	P192, P224, P256, P384, P521

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
DES_CBC_ISO9797_M1
DES_CBC_ISO9797_M2
DES_CBC_NOPAD
DES_CBC_PKCS5
DES_ECB_ISO9797_M1
DES_ECB_ISO9797_M2
DES_ECB_NOPAD
DES_ECB_PKCS5
RSA_SHA1_OAEP
RSA_SHA1_PSS
RSACRT_SHA1_OAEP
RSAES_PKCS1_OAEP_MGF1_SHA1
RSASSA_PKCS1_PSS_MGF1_SHA1
RSAES_PKCS1_V1_5 RSAES_PKCS1_OAEP_MGF1_SHA1
RSA_SHA_PKCS1
RSA_SHA1_PSS
DSA_SHA1
MD5
SHA1
HMAC_MD5
HMAC_SHA1
RSA operation with keys shorter than 2048 bits
DH operation with keys having a group shorter than 2048

2.6 Security Objectives for the Operational Environment

The Security Target establishes the following security objectives for the TOE operational environment:

OE.INTEGRATION_CONFIGURATION (defined in TEE PP)

Integration and configuration of the TEE by the device manufacturer shall rely on guidelines defined by the TEE provider that fulfill the requirements set in GlobalPlatform TEE specifications and state all the security requirements for the device manufacturer issued from the TOE evaluation.

OE.PROTECTION_AFTER_DELIVERY (defined in TEE PP)

The TOE shall be protected by the environment after delivery and before entering the final usage phase. The persons manipulating the TOE in the operational environment shall apply the TEE guidance (e.g. user and administrator guidance, installation documentation, personalization guide). 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.

Application Note:

The certificate is valid only when the guides are applied. For instance, for installation, pre-personalization or personalization guides, only the described set-up configurations or personalization profiles are covered by the certificate.

OE.ROLLBACK (defined in TEE PP)

The TA developer shall take into account that the TEE does not provide full rollback protection of TEE persistent data, TA data and keys and TA code.

In RP_SFS TOE configuration: this objective does not apply.

OE.SECRETS (defined in TEE PP)

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 (defined in TEE PP)

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.CONFIGURATION

It is assumed that the TOE will be properly configured and installed on the appropriate, dedicated hardware. The set of software packages forming the TOE must be installed during installation time in accordance with the installation instructions provided in the installation guidance document. (Kinibi Integration Guide).

OE.INITIALIZATION

It is assumed that the TOE is started through a secure initialization process starting from a non-modifiable boot code (ROM) that ensures:

the integrity of the SoC secure firmware initialization code and data used to load the SoC secure firmware;

the authenticity and rollback prevention of any secure boot stage required to initialize the TOE. (the SoC secure firmware includes all components of the secure boot chain)

the authenticity and rollback prevention of the TOE image (including Kinibi Trusted OS and embedded secure drivers).

Application Note: The fact that the process is bound to the SoC means that the root of trust for the TEE data cannot be modified or tampered with.

OE.TRUSTED_HARDWARE

SoC Hardware and secure Firmware implements the protocols and mechanisms required by the TSF to support the enforcement of the security policy. Those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results. In particular: An ARMv8 platform with REE/TEE isolation through TrustZone technology.

Hardware/Firmware are under the same management domain as the TOE, and are managed based on the same rules and policies applicable to the TOE.

OE.TRUSTED_FIRMWARE

The developers of SoC secure firmware and secure drivers are competent and trustworthy. They are capable and willing to ensure that the SoC secure firmware and the secure drivers does not break any security guarantee of the TOE, and they actually do so. Driver developers comply with the Kinibi Driver Developers Guide, in addition to the Kinibi Developers Guide which also hold for drivers.

OE.SECURE_DEBUG

The trusted platform closes any debugging facilities.

OE.UNIQUE_TEE_ID

Generation of the TEE identifier, outside or inside the TEE, shall enforce the statistical uniqueness of this data.

OE.RNG

The platform shall provide a random number generator (through the secure firmware HAL) suitable as an entropy source as specified in NIST SP 800-90A. Random numbers output by this generator is not predictable and have sufficient entropy. The SOC shall ensure that no information about the produced random numbers is available to an attacker since they might be used to generate cryptographic keys.

OE.TA_MANAGEMENT

Developers of TA management software are competent and trustworthy. They are capable and willing to ensure that the TA management software ensures that only trusted entities can deploy privileged Trusted Applications and that only the owner of a TA identity can deploy a TA bearing this identity, and they actually do so. They are capable and willing to ensure that the additional software does not break any security guarantee of the TOE, and they actually to so. Developers of TA management software comply with the TA development guidelines.

The guidance addresses the security objectives for the environment as follows:

- [Integr_guide] addresses OE.INTEGRATION_CONFIGURATION, OE.CONFIGURATION, OE.INITIALIZATION, OE.TRUSTED_HARWARE, OE.TRUSTED_FIRMWARE, OE.RNG, OE.TA_MANAGEMENT
- [Dev_guide] addresses OE.TA_DEVELOPMENT, OE.CONFIGURATION, OE.SECURE_DEBUG, OE.TA_MANAGEMENT
- [API&Driver_guide] addresses OE.TA_DEVELOPMENT
- [OP_User_guide] addresses OE.PROTECTION_AFTER_DELIVERY, OE.ROLLBACK, OE.SECRETS, OE.TA_DEVELOPMENT, OE.SECURE_DEBUG, OE.TA_MANAGEMENT

- [Prep_Procedures] addresses OE.PROTECTION_AFTER_DELIVERY, OE.ROLLBACK, OE.SECRETS, OE.TA_DEVELOPMENT, OE.CONFIGURATION, OE.INITIALIZATION, OE.TRUSTED_HARWARE, OE.TRUSTED_FIRMWARE, OE.SECURE_DEBUG, OE.UNIQUE_TEE_ID, OE.RNG, OE.TA_MANAGEMENT
- [Delivery_Guide] addresses OE.PROTECTION_AFTER_DELIVERY, OE.TA_MANAGEMENT.

2.7 Clarification of Scope

The TOE is a software TEE-part. The Security Target [ST] defines the hardware and firmware requirements for executing Kinibi 410A, which include Cortex-A73 / Cortex-A53, ARMv8-A based System-on-Chip, maximum 8 cores, ATF secure monitor in EL3, RNG and Flash memory with RPMB support in RP_SFS mode. In the Security Target, the hardware and firmware belong to the operational environment of the TOE, these are out of the scope of the evaluation.

The functional compliance of the TOE with GlobalPlatform API specification is out of the scope of the evaluation.

Trustonic's development sites as well as the procedures applicable in Phases 1 to 4 are out of the scope of the evaluation.

3 Evaluation

3.1 Evaluation Laboratory Identification

The TOE has been evaluated by Riscure B.V., located Delftechpark 49, 2628 XJ Delft, The Netherlands.

3.2 Evaluated Configuration

The evaluation addressed one version of the TOE, in two configuration modes, as defined in section 2.1. Note that any deviation from the indicated components versions brings the TOE outside the evaluated configuration.

3.3 Evaluation Activities

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

- [ST] Kinibi 410A Security Target, based on [TEE PP]
- [TEE EM] TEE Evaluation Methodology for TEE-parts
- [TEE AP] Application of Attack Potential to Trusted Execution Environment.

The evaluation activities consisted of a vulnerability analysis of the TOE based on

- Public sources
- Developer's documentation including [ST], [Integr_guide], [Dev_guide], [API&Driver_guide], [OP_User_guide], [Prep_Procedures] and [Delivery_Guide]
- Source code review for software-only attacks.

The laboratory performed the following tasks:

- Consistency check of Kinibi 410A Security Target [ST] against the TEE Protection Profile [TEE PP] (and Time & Rollback PP-Module in the RP_SFS mode)
- Consistency check between the guidance documents [Integr_guide], [Dev_guide], [API&Driver_guide], [OP_User_guide], [Prep_Procedures] and [Delivery_Guide], the security objectives for the operational environment in the [ST] and the recommendations issued from the evaluation.

Note: The laboratory also performed RNG entropy testing on Hikey960 board from 96boards implementing a Kirin 960 SoC and ARM Trusted Firmware-A v1.5 running a previous version of the product, namely Kinibi 410A V002-r0 (source code revision 87472).

3.4 Evaluation Results

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

- [DTER] Kinibi v4.10A – Security Evaluation Report, version 1.5.

The evaluation laboratory raised one security recommendation that introduces limitations on the usage of the cryptographic algorithms. This is stated as R.CRYPTO_ALG in the [ST].

The evaluation laboratory determined that:

- The Security Target [ST] is consistent[2] with the TEE Protection Profile v1.2.1, and with the Time & Rollback PP-Module in the RP_SFS mode
- All the potential vulnerabilities identified during the source code review have been either corrected, addressed by usage or testing recommendations, or considered not exploitable
- The guidance documents [Integr_guide], [Dev_guide], [API&Driver_guide], [OP_User_guide], [Prep_Procedures] and [Delivery_Guide] address all the security objectives for the operational environment listed in section 2.6 and all the usage recommendations
- The TOE is resistant to software-only attacks performed by an attacker possessing TEE-Low attack potential, as defined in [TEE PP] and [TEE AP], provided the security objectives for the operational environment and the recommendations are applied
- In the framework of a GlobalPlatform SoC or Final Device evaluation of a Kinibi 410A-based TEE, the vulnerability analysis should consider all the hardware attacks and all the hardware-based software attacks.

Note: For the reuse of Kinibi 410A evaluation results in a TEE on SoC or a TEE on Final Device evaluation conformant with GlobalPlatform TEE PP and Evaluation Methodology, the (relevant parts of) Kinibi v4.10A – Security Evaluation Report [DTER] should be made available to the laboratory.

[2] Since the TOE is a TEE-part, the ST does not claim conformance with TEE PP.

4 Certification

4.1 Usage Restrictions

The user of the certified product shall ensure that all the security objectives for the operational environment and the security recommendations stipulated in the [ST] and the guidance [Integr_guide], [Dev_guide], [API&Driver_guide], [OP_User_guide], [Prep_Procedures] and [Delivery_Guide] are fulfilled. This includes:

- OE.INTEGRATION_CONFIGURATION, OE.PROTECTION_AFTER_DELIVERY, OE.ROLLBACK (in Normal mode only), OE.SECRETS, OE.TA_DEVELOPMENT (see section 2.6)
- OE.CONFIGURATION, OE.INITIALIZATION, OE.TRUSTED_HARDWARE, OE.TRUSTED_FIRMWARE, OE.SECURE_DEBUG, OE.UNIQUE_TEE_ID, OE.RNG, OE.TA_MANAGEMENT (see section 2.6)
- R.CRYPTO_ALG (see section 2.5 and 3.4).

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 Kinibi 410A has been performed as required by the GlobalPlatform TEE Evaluation Methodology for TEE-parts [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 for software-only attacks, provided all the usage restrictions defined in section 4.1 are fulfilled. Consequently, GlobalPlatform issues the Full Certificate for Kinibi 410A in conformity with the scheme Certification Process for TEE-parts [TEE Cert Proc].

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 v1.1	[TEE Cert Proc]
GPD_SPE_021	GlobalPlatform Device Committee TEE Protection Profile v1.2.1	[TEE PP]
GPD_GUI_044	GlobalPlatform Device Technology TEE Evaluation Methodology v1.0.0.2	[TEE EM]
GPD_NOT_051	Application of Attack Potential to Trusted Execution Environment v1.5.0.10 – Confidential	[TEE AP]
GPD_SPE_010	TEE Internal Core API Specification v1.1.1	
GPD_SPE_007	TEE Internal Core API Specification v1.0	
GPD_EPR_028	TEE Client API Specification v1.0 Errata and Precisions v2.0	

Table 5-2: Product-related References and Standards

Document	Description	Ref
Security Target	Kinibi 410A Security Target, version 1.5, August 2019 SHA256(Trustonic-Kinibi-410A-ST-1.5.pdf)= 3d4ee37274cb55156777ed30fbcc86374793bec07e5ac8fb446609a582172db5	[ST]
Guidance	Kinibi Integration Manual (July 15, 2019) SHA256(Kinibi_Integration_Guide.pdf)= 72cb4e5812c4f023aa9abff0826cf32444045c18ce8dca8319a9c86068a6e6a5	[Integr_guide]
Guidance	Kinibi Developer's Guide v5.1 (Version used for the evaluation) Kinibi Developer's Guide v5.2 (editorial update requested for certification) SHA256(Kinibi_Developers_Guide.pdf)= 88fec62608162f924273428970dcb3c42f3775021e85585dd78dfc61450ea54c	[Dev_guide]

Document	Description	Ref
Guidance	Kinibi API Documentation API Level 11 (July 16, 2019), Kinibi Driver Developer's Guide v2.8 and Kinibi Driver API Documentation v2.12 SHA256(Kinibi_API_Documentation.pdf)= 76d33bab7b92472e78bfa1605ba9e0710ff04be3f92f4b37bd6f91627a52cb8d SHA256(Kinibi_Driver_API_Documentation.pdf)= 23adbc26e2a6fda04880bd953bf8ac272f0c1f27d560c9f511d5e85d7f5758d6 SHA256(Kinibi_Driver_Developers_Guide.pdf)= 59f4df902daa38c96d76ef0625163e04453682ca8d05ac1f0c5030488c0c22b7	[API&Driver_guide]
Guidance	Kinibi v410A Operational User Guidance v1.4, 2019 SHA256(Trustonic-Kinibi-AGD_OPE.pdf)= 7e4b283eeab7f8dbe58674be171b02400667fe7c986a6a817b5e91db2b29bd35	[OP_User_guide]
Guidance	Kinibi v410A Preparative Procedures Guidance v1.4, 2019 SHA256(Trustonic-Kinibi-AGD_PRE.pdf)= 5fd3490f0f9b99796d50811688eb69c80a12d736f35194e3bd01da709f021870	[Prep_Procedures]
Guidance	ALC_DEL - Kinibi Delivery v1.2, 2019 SHA256(Trustonic-Kinibi-ALC_DEL.pdf)= f406c2a6c2a789b3ccd8fe9d229e432e8a7841bf23f432fac2ee5082638af45d	[Delivery_Guide]
Evaluation Report	Kinibi v4.10A – Security Evaluation Report, version 1.5. SHA256(2018133-D1 Trustonic Kinibi Security Evaluation Report 1.5.pdf)= 55f0d0ac99d9288202e4d4d5842cac1874fc59be06dd9540947894ad1262598e	[DTER]
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	

Document	Description	Ref
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
HAL	Hardware Abstraction Layer
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
RPMB	Replay Protected Memory Block
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

Mounji Methlouthi

Signature numérique de Mounji Methlouthi
DN : c=US, cn=Mounji Methlouthi, email=mounji.methlouthi@smart-consulting.com
Date : 2019.12.05 04:22:40 +01'00'