GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certificate of Security Evaluation

Samsung TEEgris v4.1 on Exynos 990/980 devices

Certification Number:	GP-TEE-2020/01
Issuance Date:	September 22, 2020
Sponsor:	Samsung Electronics Co., Ltd
Protection Profile:	TEE PP v1.2.1 – Base PP
PP-Modules:	☑ Debug v1.2.1
Product Type:	☑ TEE on Final Device
	☐ TEE on SoC
	☐ TEE partial scope
Evaluation Type:	☑ Full ☐ Delta ☐ Fast-track
Security Evaluation Lab:	Thales ITSEF (Labège, France)
Certification Type:	☑ Full ☐ Restricted
Certification Report:	GP-TEE-2020/01-CR

Product Name:	Samsung TEEgris v4.1
Developer:	Samsung Electronics Co., Ltd
Trusted OS:	Samsung Secure OS (TEEgris) v4.1.0.0
SoC / devices:	Exynos 990 for devices:
	• Samsung Galaxy S20 (SM-G980F, SM-G981B)
	• Samsung Galaxy S20+ (SM-G985F, SM-G986B)
	• Samsung Galaxy S20 Ultra (SM-G988B)
	• Samsung Galaxy Note 20 (SM-N980F, SM-N981B)
	• Samsung Galaxy Note 20 Ultra (SM-N985F, SM-N986B)
SoC / devices:	Exynos 980 for devices:
	• Samsung Galaxy A71 5G (SM-A7160, SM-A716B, SM-A716S)
	• Samsung Galaxy A51 5G (SM-A5160, SM-A516B, SM-A516N, SM-A516U)

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 Directeur

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

GLOBALPLATFORM®
CERTIFIED TEE

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform TEE Security Evaluation Secretariat
Certification Report
GP-TEE-2020/01-CR v1.1

Issue date:	2022.03.24 (v1.1) / 2020.09.22 (v1.0)
Products:	Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 990 for devices: - Samsung Galaxy S20 (SM-G980F and SM-G981B) - Samsung Galaxy S20+ (SM-G985F and SM-G986B) - Samsung Galaxy S20 Ultra (SM-G988B) - Samsung Galaxy Note 20 (SM-N980F and SM-N981B) - Samsung Galaxy Note 20 Ultra (SM-N985F and SM-N986B) Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 980 for devices: - Samsung Galaxy A71 5G (SM-A7160, SM-A716B and SM-A716S) - Samsung Galaxy A51 5G (SM-A5160, SM-A516B, SM-A516N and SM-A516U)
Sponsor and Developer:	Samsung Electronics - Mobile Communication Division 129, Samsung- ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Korea
Laboratory:	Thales ITSEF - 290 allée du Lac, 31670 Labège, France
Conformance:	☑ TEE PP v1.2.1 – Base PP ☑ Debug PP-Module
Product Type:	☑ TEE on Final Device (family of products) ☐ 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

1 Executive Summary 5

2 Products 6

2.1 Identification 6
2.2 Documentation 8
2.3 Architecture 8
2.4 Life-cycle 10
2.5 Security Functionality 10
2.6 Assumptions 12
2.7 Clarification of Scope 14

3 Evaluation 15

3.1 Evaluation Laboratory Identification 15
3.2 Evaluated Configuration 15
3.3 Evaluation Activities 15
3.4 Evaluation Results 16

4 Certification 17

4.1 Usage Restrictions 17
4.2 Conclusion 17

5 References 18

6 Abbreviations 21

Tables

Table 2-1: Identification of Exynos 990 family of products 6

Table 2-2: Identification of Exynos 980 family of products 6

Table 2-3: Identification of TOE components for Exynos 990 family 6

Table 2-4: Identification of TOE components for Exynos 980 family 7

Table 2-5: Identification of TAs for Exynos 990 and Exynos 980 families 7

Table 2-6: TOE cryptographic algorithms 11

Table 5-1: Samsung Electronics References 18

Table 5-2: GlobalPlatform References 18

Table 5-3: External references 19

Table 6-1: Abbreviations 21

1 Executive Summary

This document constitutes the Certification Report for the evaluation of two families of products developed by Samsung Electronics, registered under number GP200007:

- *Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 990* for devices*:*
    - Samsung Galaxy S20 (SM-G980F and SM-G981B)
    - Samsung Galaxy S20+ (SM-G985F and SM-G986B)
    - Samsung Galaxy S20 Ultra (SM-G988B)
    - Samsung Galaxy Note 20 (SM-N980F and SM-N981B)
    - Samsung Galaxy Note 20 Ultra (SM-N985F and SM-N986B)
- *Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 980* for devices*:*
    - Samsung Galaxy A71 5G (SM-A7160, SM-A716B and SM-A716S)
    - Samsung Galaxy A51 5G (SM-A5160, SM-A516B, SM-A516N and SM-A516U)

The type of TOE is a Trusted Execution Environment (TEE) on Final Device.

The evaluation has been performed by the accredited laboratory Thales ITSEF in Labège (France). The following documents constitute the basis for this evaluation: *Samsung TEEgris Security Target, version 1.2, 2020-08-26* [ST] and *Samsung TEEGRIS, Security Architecture v4.x 2020-02-18* [Guide].

The evaluation has been conducted in three steps:

- Full evaluation of TEE on Final Device Samsung Galaxy S20+ (SM-G986F)
- Delta evaluation of TEE on Final Device Samsung Galaxy A71 5G (SM-A7160)
- Impact analysis for the other target Final Devices.

The evaluation determined that the two families of products that are identified in this certification report meet the GlobalPlatform TEE security functional requirements stated in the Security Target *[ST]* at the assurance level AVA_TEE.2 and that the guidance *[Guide]* 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 two technical evaluation reports:

- *GP Detailed TEE Evaluation Report, Project: TEEGRIS 4.1 on Exynos 990*, version 1.2
- *GP Detailed TEE Evaluation Report, Project: TEEGRIS 4.1 on Exynos 980*, version 1.2.

The certification determined that the evaluation has been performed in conformance with *GlobalPlatform TEE Protection Profile v1.2.1* with *Debug PP-Module* [TEE PP] and *TEE Evaluation Methodology v1.0.0.0* [TEE EM]. The certificate is valid provided all the usage restrictions defined in section 4.1 are fulfilled.

Remarks:

The present Certification Report v1.1 cancels and replaces the Certification Report v1.0. It clarifies the scope of the evaluation and certification, which does not include the pre-loaded TAs.

2 Products

2.1 Identification

The Products in this evaluation are two TEE families developped by Samsung Electronics:

Table 2-1: Identification of Exynos 990 family of products

Product Identification for Exynos 990 family	
Product name	Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 990
Developer	Samsung Electronics
Product type	TEE on Final Device
Final device models	Samsung Galaxy S20 (SM-G980F and SM-G981B) Samsung Galaxy S20+ (SM-G985F and SM-G986B) Samsung Galaxy S20 Ultra (SM-G988B) Samsung Galaxy Note 20 (SM-N980F and SM-N981B) Samsung Galaxy Note 20 Ultra (SM-N985F and SM-N986B)
Tested device	Samsung Galaxy S20+ (SM-G986F)

Table 2-2: Identification of Exynos 980 family of products

Product Identification for Exynos 980 family	
Product name	Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 980
Developer	Samsung Electronics
Product type	TEE on Final Device
Final device models	Samsung Galaxy A71 5G (SM-A7160, SM-A716B and SM-A716S) Samsung Galaxy A51 5G (SM-A5160, SM-A516B, SM-A516N and SM-A516U)
Tested device	Samsung Galaxy A71 5G (SM-A7160)

The Target of Evaluation (TOE) for each product family consists of the set of components that are listed in the following tables:

Table 2-3: Identification of TOE components for Exynos 990 family

TOE Components Identification for Exynos 990 family		**Developer**
ROM code	Tokyo-QP1A-9C19R1 SHA256: 219f79842288ec957b52785291e4b55554d969613fb5e1bab4552c3b662cc88a	Samsung Electronics
Pre-Loader boot code	Same as ROM code	Samsung Electronics

ATF	v1.5 SHA256: 1cf2aea7eb609417e4e3bfdb408601fdbf0889806a50ada3d3ab957faab47914	Samsung Electronics
Trusted OS binary	Samsung Secure OS Release Version 4.1.0.0SHA256: 28f59679b68c101176f707fe422237a17b6ccb31fca159bdfa791b19b1dcd7a4	Samsung Electronics
Pre-loaded TAs	Keymaster, Gatekeeper, Key management, TIMA, Biometric, DRM, Trusted user interface, Authentication, Data management, Samsung Payment See identification data below.	Samsung Electronics

Table 2-4: Identification of TOE components for Exynos 980 family

TOE Components Identification for Exynos 980 family		**Developer**
ROM code	Paris-QQ1A-9C02R1 SHA256: d2f6cf33d0f086585085ecc2b6ad59934e9ff567274e66d6f8a96ade534c708f	Samsung Electronics
Pre-Loader boot code	Same as ROM code	Samsung Electronics
ATF	v1.5(release): Paris-QQ1A-9C02R1 SHA256: 39844559fc0e2599c69de9f2eb4d9236e8ded74e726cc31b2d5f5acd9d875565	Samsung Electronics
Trusted OS binary	Samsung Secure OS Release Version 4.1.0.0 SHA256: e1fb44a323ad1dc5788f2bfb7027ae2ba61b669e44507452404f9d959f150e45	Samsung Electronics
Pre-loaded TAs	Keymaster, Gatekeeper, Key management, TIMA, Biometric, DRM, Trusted user interface, Authentication, Data management, Samsung Payment. See identification data below.	Samsung Electronics

The two families of products contain the following TAs, which are not part of nor involved in the TOE Security Functionality (TSF). Table 2-5: Identification of TAs for Exynos 990 and Exynos 980 families

TA Identification for Exynos 990 and Exynos 980 families		**Developer**
Pre-loaded TAs	Keymaster 00000000-0000-0000-0000-4b45594d5354 00000000-0000-0000-0000-534258505859 00000000-0000-0000-0000-53626f786476	Samsung Electronics
	Gatekeeper (driver) 00000000-0000-0000-0000-474154454b45	
	Key management 00000000-0000-0000-0000-000000534b4d 00000000-0000-0000-0000-505256544545 00000000-0000-0000-0000-0000534b504d	

TA Identification for Exynos 990 and Exynos 980 families		Developer
	TIMA (attestation, keystore) 00000000-0000-0000-0000-00000000dead 00000000-0000-0000-0000-00535453540b 00000000-0000-0000-0000-00535453540c 00000000-0000-0000-0000-0053545354ab	
	Biometric (face, fingerprint) (driver) 00000000-0000-0000-0000-42494f535542 00000000-0000-0000-0000-46494e474502 00000000-0000-0000-0000-5345435f4652	
	DRM (widevine, hdcp) (driver) 00000000-0000-0000-0000-00575644524d 00000000-0000-0000-0000-000048444350	
	Trusted user interface (driver) 00000000-0000-0000-0000-000000010081 00000000-0000-0000-0000-000000020081	
	Authentication (driver) 00000000-0000-0000-0000-0050524f4341	
	Data management 00000000-0000-0000-0000-564c544b5052 00000000-0000-0000-0000-564c544b4456	
	Samsung Payment 00000000-0000-0000-0000-00504159544D 00000000-0000-0000-0000-504159415554 00000000-0000-0000-0000-564953415059 00000000-0000-0000-0000-4D4153545059 00000000-0000-0000-0000-414D45585059	

The Rich OS (Android Q and TEE Client APIs) are non-TOE components which are required for the operation of the TOE for both product families.

2.2 Documentation

The Security Target for this evaluation is:

- [ST] *Samsung TEEgris Security Target, version 1.2, 2020-08-26.*

The guidance for application developers consists of the following documents:

- [Guide] *Samsung TEEGRIS, Security Architecture v4.x 2020-02-18*.

2.3 Architecture

The hardware architecture of the two families of products consists of:

- Hardware processing unit (with Security Extension and 8 cores):
    - For Exynos 990 family: ARMv8 A55, A76 and M5 Processor
    - For Exynos 980 family: ARMv8 A55, Deimos(A77custom) Processor
- Physical volatile memory: Secure DRAM (75MB external DRAM reserved for Secure OS) and Secure Internal SRAM:
    - For Exynos 990 family: external DRAM hardware module on top of the SoC (PoP package)
    - For Exynos 980 family: external DRAM hardware module soldered aside the SoC
- Physical non-volatile memory: Secure BROM, Efuse (Secure OTP)
- Memory Protection Unit (MPU) as hardware solution for definition and isolation of memory areas
- Secure peripherals:
    - Accessible from Secure World only: Secure JTAG, PRNG/TRNG, Secure Timer, Secure Watchdog, CryptoEngine (AES, SHA256, and RSA)
    - Shared with Normal World (the hardware instance can be switched between controls under Secure and Normal Worlds depending on the current session): SD/MMC, eMMC or UFS, USB20, UARTs, I2Cs, Timers, SPI, KEYPAD, GPIO, Watchdog, GPU, Video Encode, Video Decode, ISP, and Display Controller
- Connections between the processing unit(s) and the hardware resources: AXI-based Bus.

The software architecture of the two families of products consists of ROM boot code, Pre-loader, ATF, Samsung Secure OS (TEEgris) v4.1.0.0 and the pre-loaded Trusted Applications.

The TOE provides the following software interfaces:

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

The TOE implements the following GlobalPlatform APIs, for which Samsung Electronics declares 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
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
GPD_SPE_020	Trusted User Interface API Specification	1.0

The TOE implements the following GlobalPlatform APIs, for which Samsung Electronics declares partial functional compliance in the Security Target.

Reference	Declarative Partial Compliance	Version
GPD_SPE_024	TEE Secure Element API Specification	1.0
GPD_EPR_030	TEE Secure Element API Specification 1.0 Errata and Precisions	1.0
GPD_SPE_025	TEE TA Debug Specification	1.0

The TOE also implements the following Proprietary APIs, defined by Samsung Electronics:

Reference	Developer	Version	Content
[SMGAPI]	Samsung Electronics	4.0	Samsung Internal API reference

The TOE does not include the Rich Execution Environment (REE) which consists of Android Q (including the TEE client APIs) and the applications running on top.

2.4 Life-cycle

The TOE life cycle is split in 6 development and manufacturing phases plus the end-user phase:

- [Samsung Electronics] Phase 1 corresponds to the TEE firmware & hardware design
- [Samsung Electronics] Phase 2 corresponds to the SoC manufacturing
- [Samsung Electronics] Phase 3 corresponds to TEE software design
- [Samsung Electronics] Phase 4 corresponds to TEE software integration
- [Samsung Electronics] Phase 5 corresponds to TEE integration with SoC
- [Samsung Electronics] Phase 6 corresponds to the device manufacturing. In this phase, the TEE is initialized and personalized, before delivery
- Phase 7 stands for the end-usage of the device.

The TOE is delivered as a final device at the end of Phase 6.

2.5 Security Functionality

The security functionality of the TOE in the end-user phase, for the two families, 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:
    - Cryptographic structure ensuring confidentiality, integrity and binding to the TEE
    - Monitoring action ensuring consistency and atomicity

    - Violation action ensuring integrity and rollback attempts at-runtime
- Random Number Generator (DRBG NIST SP800-90A)
- Cryptographic API (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, downgrade of TA code and binary
- Irreversible JTAG configurations for debug access:
    - Access control based on cryptographic authentication on final product.

The TOE relies on the following cryptographic functionality:

- ECDSA 384 signature verification of TEE firmware upon initialization, based on hardware root of trust
- RSA PKCS 1.5 2048 signature verification of TA code upon application instantiation (loading), based on OEM certificate
- AES-GCM 256 encryption/decryption of stored TA data, based on hardware root-of-trust for Trusted Storage, diversified per TA.

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

Table 2-6: TOE cryptographic algorithms

Category	**Algorithm identifier**	**Key length (bits)**
AES	AES_ECB_NOPAD, AES_CBC_NOPAD, AES_CTR, AES_CTS, AES_CBC_MAC_NOPAD, AES_CBC_MAC_PKCS5, AES_CBC_MAC_ISO9797_M2, AES_CMAC, AES_CCM, AES_GCM, AES_ECB_ISO9797_M1, AES_ECB_ISO9797_M2, AES_CBC_ISO9797_M1, AES_CBC_ISO9797_M2, AES_ECB_PKCS5, AES_ECB_PKCS7, AES_CBC_PKCS5, AES_CBC_PKCS7PKCS5, AES_CMAC AES_XTS (only 128 and 256 bit key length)	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	Up to 4096 bits

Category	Algorithm identifier	Key length (bits)
RSA Encryption	RSAES_PKCS1_V1_5, RSAES_PKCS1_OAEP_MGF1_SHA224, RSAES_PKCS1_OAEP_MGF1_SHA256, RSAES_PKCS1_OAEP_MGF1_SHA384, RSAES_PKCS1_OAEP_MGF1_SHA512, RSA_NOPAD (Encryption)	Up to 4096 bits
DSA	DSA_SHA224, DSA_SHA256	
DH	DH_DERIVE_SHARED_SECRET	
Hash	SHA224, SHA256, SHA384, SHA512	-
HMAC	HMAC_SHA224, HMAC_SHA256, HMAC_SHA384, HMAC_SHA512	-
ECDSA	ECDSA	P224, P256, P384, P521
ECDH	ECDH	P224, P256, P384, P521

The following recommendation 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:

- DES-based algorithms (all)
- RSASSA_PKCS1_V1_5_SHA1
- RSASSA_PKCS1_PSS_MGF1_SHA1
- RSAES_PKCS1_OAEP_MGF1_SHA1
- DSA_SHA1
- SHA1
- HMAC_SHA1
- RSA with keys shorter than 2048 bits
- DH with keys having a group shorter than 2048.

2.6 Assumptions

The Security Target establishes the following assumptions, which apply to the two TOE families:

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.

Note: The assumption A.PROTECTION_AFTER_DELIVERY is included in the [ST] for completeness with regard to the TEE PP only, since the TOE is delivered to the end user and no specific guidelines apply.

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.ROLLBACK

It is assumed that TA developers do not rely on protection of TA data and keys trusted storage against full rollback.

Note: the assumption A.ROLLBACK defined in the TEE PP[1] has been updated in the [ST] to reflect the fact that the TOE does protects the integrity of the TEE persistent data and TA code.

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 a TA Authority ID (if define) 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 life-cycle and of TA persistent data life-cycle within the TA itself.

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 signature keys without authorization.

[1] (In TEE PP) A.ROLLBACK It is assumed that TA developers do not rely on protection of TEE persistent data, TA data and keys and TA code against full rollback.

2.7 Clarification of Scope

This is a TEE on Final Device evaluation for two families of products on several device models (cf. section 2.1), therefore the scope of the evaluation includes the SoC and the external memory.

The functionality of the pre-loaded TAs identified in section 2.1, which include the management of the Trusted User Interface and the biometric interface of the device, is out of the evaluation scope.

The source code of Samsung Secure OS (TEEgris) v4.1.0.0 is the same for the Exynos 990 and Exynos 980 families of devices. There is only one configuration for the TOE for the two families applicable to all the identified final devices.

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.

Samsung Electronics 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 TOE has been evaluated by Thales ITSEF, located 290 allée du Lac, 31670 Labège, France.

3.2 Evaluated Configuration

The evaluation addressed two families of products, as defined in section 2.1:

- The Exynos 990 family was tested on Samsung Galaxy S20+ (SM-G986F)
- The Exynos 980 family was tested on Samsung Galaxy A71 5G (SM-A7160).

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 GlobalPlatform documentation:

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

The evaluation has been conducted in three steps:

- Full evaluation of TEE on Final Device Samsung Galaxy S20+ (SM-G986F)
- Delta evaluation of TEE on Final Device Samsung Galaxy A71 5G (SM-A7160) based on the Samsung Galaxy S20+ evaluation
- Impact analysis for the other target Final Devices identified in Table 2-1 and Table 2-2.

The evaluation activities consisted of:

- Vulnerability analysis of the TOE based on public sources and on developer's documentation including [ST], [SMGAPI] and [Guide]
- Source code review of the TOE's software components including secure boot, Trusted OS, GlobalPlatform APIs and Samsung APIs
- Quality testing of random numbers generated by the TOE
- Software and hardware-based TOE penetration testing on:
  - Samsung Galaxy S20+ (SM-G986F) for Exynos 990 family
  - Samsung Galaxy A71 5G (SM-A7160) for Exynos 980 family.

The laboratory has also performed the following tasks:

- Conformity check of the Security Target [ST] against the TEE Protection Profile with Debug PP-Module [TEE PP]

- Consistency check between the guidance [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 two technical reports:

- [DTER 990] *GP Detailed TEE Evaluation Report, Project: TEEGRIS 4.1 on Exynos 990,* version 1.2
- [DTER 980] *GP Detailed TEE Evaluation Report, Project: TEEGRIS 4.1 on Exynos 980*, version 1.2.

One limitation on the usage of TOE is given in **R.CRYPTO_ALG,** which lists the cryptographic APIs that are not in the scope of the certificate and should not be used.

The evaluation laboratory determined that:

- The Security Target [ST] is conformant to the TEE Protection Profile v1.2.1 with Debug PP-Module
- The TOE successfully passed the 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 guidance [Guide] addresses 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 products must ensure that all the following assumptions and security recommendations stipulated in the Security Target [ST] and the guidance [Guide] are fulfilled:

- A.PROTECTION_AFTER_DELIVERY, A.TA_DEVELOPMENT, A.ROLLBACK, 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 made available to the users of the certified products. 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 products.

4.2 Conclusion

This certification report confirms that the evaluation of the two families of products complies with GlobalPlatform requirements and that there is sufficient evidence to affirm that the products meet the Security Target [ST] and the AVA_TEE.2 requirements, provided all the usage restrictions defined in section 4.1 are fulfilled.

Consequently, GlobalPlatform issues the Full Certificate for the two families of products:

- Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 990 family for devices:
  - Samsung Galaxy S20 (SM-G980F and SM-G981B)
  - Samsung Galaxy S20+ (SM-G985F and SM-G986B)
  - Samsung Galaxy S20 Ultra (SM-G988B)
  - Samsung Galaxy Note 20 (SM-N980F and SM-N981B)
  - Samsung Galaxy Note 20 Ultra (SM-N985F and SM-N986B)
- Samsung Secure OS (TEEgris) v4.1.0.0 on Exynos 980 family for devices:
  - Samsung Galaxy A71 5G (SM-A7160, SM-A716B and SM-A716S)
  - Samsung Galaxy A51 5G (SM-A5160, SM-A516B, SM-A516N and SM-A516U)

in conformity with the Certification Process [TEE Cert Proc].

The user of the certified products 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.

Guillaume ACHTEN
Process Owner

Guillaume Achten

Digitally signed by Guillaume Achten
DN: c=US, st=California, l=Redwood City, o=GLOBALPLATFORM, INC., cn=Guillaume Achten, email=guillaume.achten@mellonne.com
Date: 2022.03.24 13:56:54 +01'00'

5 References

Table 5-1: Samsung Electronics References

Document	Description	Ref
Security Target	Samsung TEEgris Security Target, version 1.2, 2020-08-26 SHA256(Samsung_TEEgris_Security_Target_v1.2_submission(clean).pdf)= a3aa4f258fb6b63a801cfd0ab87ec8f212f4f22724ccf24a636a202352d03a83	[ST]
API	Samsung Internal API reference v4.0	[SMGAPI]
Guidance	Samsung TEEGRIS, Security Architecture v4.x 2020-02-18 SHA256(Samsung_TEEGRIS_Security_Architecture.pdf)= 7e7d543b32da945d5ddeb92a190148de9bca60574fdb08e4fcabaae3386374ed	[Guide]
Evaluation Report	GP Detailed TEE Evaluation Report, Project: TEEGRIS 4.1 on Exynos 990, version 1.2. SHA256(TEEGRIS4-1-990_GP_ER_v1.2_GlobalPlatform Security Evaluation Secretariat.pdf)= 8e2db35b85b049fe5b668303a6b2204afbc962274cbc5d3594f5df2c4d5bdd95	[DTER 990]
Evaluation Report	GP Detailed TEE Evaluation Report, Project: TEEGRIS 4.1 on Exynos 980, version 1.2. SHA256(TEEGRIS4-1-980_GP_ER_v1.2_GlobalPlatform Security Evaluation Secretariat.pdf)= 23cffd75e0f8ecf1c983bf9c3304eac5629a1df7de96d9cfc420d5dfa1dfccb2	[DTER 980]

Table 5-2: 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 v1.0.0.0	[TEE EM]
GPD_NOT_051	Application of Attack Potential to Trusted Execution Environment v1.5.0.13 – Confidential	[TEE AP]
GPD_SPE_007	TEE Client API Specification v1.0	
GPD_EPR_028	TEE Client API Specification v1.0 Errata and Precisions v2.0	
GPD_SPE_010	TEE Internal Core API Specification v1.1	
GPD_EPR_017	TEE Internal Core API Specification v1.0 Errata and Precisions v1.0 TEE Internal Core API Specification v1.0 Errata and Precisions v3.0	

Document	Description	Ref
GPD_SPE_020 GPD_SPE_024	Trusted User Interface API Specification v1.0 TEE Secure Element API Specification v1.0	
GPD_EPR_030	TEE Secure Element API Specification 1.0 Errata and Precisions v1.0	
GPD_SPE_025	TEE TA Debug Specification v1.0	

Table 5-3: External references

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	

Document	Description	Ref
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
API	Application Programming Interface
ARM	Advanced RISC (Reduced Instruction Set Computer) Machine
ATF	ARM Trusted Firmware
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
TSF	TOE Security Functionality
TRNG	True RNG