GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certificate of Security Evaluation

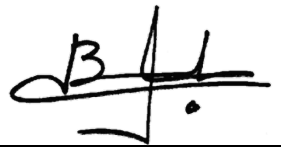
WatchTrust 2.1.1 on SC9860

Certification Number:	**GP-TEE-2018/01**
Issuance Date:	**September 4th 2018**
Sponsor:	**Watchdata**
Protection Profile:	**TEE PP v1.2.1 – Base PP**
Certification Type:	**Full**
Certification Report Number:	**GP-TEE-2018/01-CR**

Product Name:	**WatchTrust 2.1.1 on SC9860**
Product References:	**Watchdata Secure OS WatchTrust 2.1.1** **Spreadtrum SoC SC9860**
Developers:	**Watchdata** **Spreadtrum Communications, Inc.**
Product Type:	**TEE on SoC**
Evaluation Type:	**Full**
Security Evaluation Lab:	**Beijing ZhiHuiYunCe (DPLS Lab) Equipment Technology Co., Ltd.**

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-2018/01-CR v1.0

Issue date:	2018.09.04
Product:	WatchTrust 2.1.1 on SC9860
Sponsor:	Watchdata
Developer(s):	Watchdata 8F, West of Qiming International Mansion, No. 101 Lize Middle Park, Wangjing, Chaoyang District, Beijing, P.R. China Spreadtrum Communications, Inc 5th Floor Block B, No.7 Zhichun Road, Haidian District, Beijing, P.R. China
Laboratory:	Beijing ZhiHuiYunCe (DPLS Lab) Equipment Technology Co., Ltd. Room 701, building 7, No. 98, West Lake, Mentougou District, 102308, Beijing, China
Conformance:	TEE PP v1.2.1 – Base PP
Product Type:	TEE on SoC
Certification Type:	Full

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 *WatchTrust 2.1.1 on SC9860*, developed by Watchdata and Spreadtrum Communications, Inc, registered under number GP170003.

The evaluation has been performed by accredited laboratory DPLS Lab in Beijing (China). The following documents constitute the basis for this evaluation: *Watchdata TEE (WatchTrust) Security Target v1.3.3*, *WatchTrust Integration Guide for Spreadtrum v1.1*, *WatchTrust Developer's Guide v1.3*, and *WatchTrust Final Users Guide v1.1*.

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 *Watchdata GP170003 Detailed Technical Evaluation Report_V10*, version 1.0, amended with *Watchdata GP170003 Detailed Technical Evaluation Report_V10 Annex,* version 2.0.

The certification determined that the evaluation has been performed in conformance with GlobalPlatform TEE Protection Profile v1.2.1 and TEE Evaluation Methodology v1.0. 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 WatchTrust 2.1.1 on SC9860, developped by Watchdata and Spreadtrum Communications, Inc:

Product Identification	
Product Name:	Watchtrust 2.1.1 on SC9860
Developers:	Watchdata 8F, West of Qiming International Mansion, No. 101 Lize Middle Park, Wangjing, Chaoyang District, Beijing, P.R. China Spreadtrum Communications, Inc 5th Floor Block B, No.7 Zhichun Road, Haidian District, Beijing, P.R. China
Product Type:	☑ TEE on SoC

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:	Spreadtrum Communications Whale2_sp9860g	Spreadtrum
ROM code:	Whale2_9860_IROM_Code_Version_1.1.0	Spreadtrum
Pre-Loader boot code:	Whale2_9860_SPL _Version_2.1.0 – SHA-256**:** bd9d1e0c783505c7244c1fdafd452ef7cca4f1ecfa2a4d1a22154f22344d4204	Spreadtrum
SML binary (ATF):	Whale2_9860_SML _Version_2.2.0 – SHA-256: b892d23e546766f78b4470c8bafcceb0c2b6a4248d730a307ae314d889787048	Spreadtrum /Watchdata
TEE binary:	WatchTrust v2.1.1 on SC9860 – SHA-256: 620f0cdc6df43f54329117517b1af7b7782f6cfd4900a968ea4c02b565b3611c	Watchdata

The TEE Product does not comprise any pre-loaded application.

The Rich OS (Android Marshmallow, 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] *Watchdata TEE(Watchtrust) Security Target, ref. WD_SE_001,* version 1.3.3

The ST is compliant with TEE Protection Profile v1.2.1 – Base PP, i.e. without "Time & Rollback" and "Debug" PP-Modules.

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

- [Integr_guide] *WatchTrust Integration Guide for Soreadtrum*, ref. WD_WT_001, version 1.1;
- [Dev_guide] *WatchTrust Developer's Guide*, ref. WD_WT_002, version 1.3;
- [Final_guide] *WatchTrust Final Users Guide*, ref. WD_WT_003, version 1.1.

2.3 Architecture

The hardware architecture of the TOE consists of Spreadtrum SoC SC9860, which is an 8-core ARM v8 A53 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 TEE OS, e.g. JTAG.

Note: The External DRAM hardware module is not part of the SoC.

The software architecture of the TOE consists of ROM boot code, Pre-loader (SPL binary), ATF (SML binary), and Watchdata's Secure OS WatchTrust 2.1.1

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

The TOE provides the following software interfaces:

- A proprietary communication interface with the REE;
- A proprietary low-level interface for TA-TEE and TA-TA communication;
- GlobalPlatform API (see below);
- Other APIs (see below).

The TOE implements the GlobalPlatform API listed below, for which Watchdata 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	1.0
	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

The TOE also provides the following Proprietary APIs, developed by Watchdata and Spreadtrum:

Reference	Developper	Version	Content
[WGPIOAPI]	Watchdata	1.0	Watchdata GPIO and SPI API
[SAPI]	Spreadtrum	1.0	Spreadtrum Secure boot API (Functions for the modem code integrity validation)
[TAAPI]	Watchdata	1.0	Watchdata TA management API

The TOE includes as well the following NICTA's Libraries (open source code):

Library	Developper	Version	Content
datastruct	NICTA	2.0	Provides simple C data structures such as vectors, hash tables and allocation tables.
refos	NICTA	2.0	RPC specifications and generated stubs and low-level helper libraries
refossys	NICTA	2.0	Implements some POSIX system calls using low-level OS and thus allows the C library to work
platsupport	NICTA	2.0	Device interfaces, includes chardev, delay, io, serial timer
muslc	NICTA	2.0	Implementation of the standard C library targeting the Linux syscall API

2.4 Life-cycle

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

- [Spreadtrum] Phase 1 corresponds to the hardware design including the ROM code and REE development;
- [Watchdata] Phase 2 corresponds to the TEE firmware design and development;
- [Watchdata] Phase 3 corresponds to TEE firmware porting and delivery;
- [Spreadtrum] Phase 4 corresponds to the Device production with TEE software integration, including SoC personalization;
- Phase 5 stands for the end-usage of the device.

The TOE operational phase starts in Phase 4.

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 TAs from the REE;
- Isolation between Trusted Applications and isolation of the TEE from the TAs;
- Protected communication interface between Client Applications (CAs) in the REE and TAs in the TEE;
- Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE;
- Random Number Generator (TRNG and DRBG which uses the NIST SP800-90A approved algorithm for generating the random numbers based on the seed);
- Cryptographic API for TAs (see below);
- TA instantiation that ensures the authenticity and contributes to the integrity of the TA code;

- Monotonic TA instance time;
- Correct execution of TA services;
- TEE firmware integrity verification;
- Prevention of downgrade of TEE firmware;
- Debug mode not activated on production devices.

The TOE relies on the following cryptographic functionality:

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

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

Category	**Algorithm identifier**	**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, 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 2048
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	up to 2048
DSA	DSA_SHA224	2048
	DSA_SHA256	2048, 3072
DH	DH_DERIVE_SHARED_SECRET	256 to 2048
Hash	SHA224, SHA256, SHA384, SHA512	-
HMAC	HMAC_SHA224, HMAC_SHA256, HMAC_SHA384, HMAC_SHA512	-
ECDSA	ECDSA	up to 521
ECDH	ECDH_DERIVE_SHARED_SECRET	up to 521

The following recommendation for TA developers applies:

R.CRYPTO_ALG:

Although GlobalPlatform specification requires the implementation of the following algorithms, these are not in the scope of the evaluation and their usage is not recommended:

Not recommended algorithms
DES_CBC_NOPAD
DES_CBC_MAC_NOPAD
DES_CBC_MAC_PKCS5
DES_ECB_NOPAD
DSA_SHA1
HMAC_MD5
HMAC_SHA1
MD5
RSASSA_PKCS1_V1_5_MD5
RSASSA_PKCS1_V1_5_SHA1
RSASSA_PKCS1_PSS_MGF1_SHA1
RSAES_PKCS1_OAEP_MGF1_SHA1
SHA1

2.6 Assumptions

The Security Target of WatchTrust 2.1.1 on SC9860 establishes the following assumptions:

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.ROLLBACK (from TEE PP)

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.

A.SOC_PACKAGE

It is assumed that CPU and DRAM are grouped together by a POP package in the devices.

A.TA_MANAGEMENT

It is assumed that TA developers are aware of the TA life cycle and Trusted Storage principles, namely:

- TA single-instance model;
- Implicit TA install at load time upon TA session opening, provided no TA instance with the same identity is running and the TA signature is correct;
- Implicit TA uninstall when the TA instance dies;
- Ownership of the persistent data stored in the Trusted Storage associated with a given TA identity is automatically granted to any application instance that is loaded with such TA identity;
- TEE does not erase any TA persistent data from the Trusted Storage which 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.

Remark: Note that TA identification (or TA identity) consists of a TA UUID which is the name of the TA's binary.

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.

The guidance addresses the assumptions:

- [Integr_guide] covers A.PROTECTION_AFTER_DELIVERY and A.SOC_PACKAGE;
- [Dev_guide] covers A.TA_DEVELOPMENT, A.ROLLBACK, A.TA_MANAGEMENT and A.UUID_MANAGEMENT.

2.7 Clarification of Scope

The External DRAM hardware module is a non-TOE component, which is out of the evaluation scope. However, the CPU and the DRAM are expected to be integrated into a PoP Package.

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.

Spreadtrum and Watchdata development and manufacturing 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 DPLS Lab, located Room 701, building 7, No. 98, West Lake, Mentougou District, 102308, Beijing, China.

3.2 Evaluated Configuration

The evaluation addressed one TEE Product configuration, defined by the TOE and non-TOE components identified in section 2.1. Note that any deviation from the indicated components versions may bring the TOE outside the evaluated configuration.

The testing of the TOE has been performed on Spreadtrum devices embedding the WatchTrust 2.1.1 on SC9860 components, in two operation modes:

- Development mode, with activated debug features and root privilege;
- Production mode.

3.3 Evaluation Activities

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

- [TEE PP] TEE Protection Profile, reference GPD_SPE_021, version 1.2.1;
- [TEE EM] TEE Evaluation Methodology, reference GPD_GUI_044, version 1.0;
- [TEE CAT] TEE Common Automated Tests, reference GPD_SPE_050, version 1.0 as amended by TEE Security Test Suite, version 1.0.2;
- [TEE AP] Application of Attack Potential to Trusted Execution Environment, reference GPD_NOT_051, version 1.4.0.

The evaluation activities consisted of:

- Vulnerability analysis of the TOE based on public sources and on developer's documentation including [ST], [Integr_Guide], [Dev_guide] and [Final_guide];
- Source code review of the TOE's software components;
- Testing of the GlobalPlatform TEE Internal Core API against the TEE Security Test Suite v1.0.2;
- 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], [Dev_guide] and [Final_guide], the assumptions 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] *Watchdata GP170003 Detailed Technical Evaluation Report,* Version 1.0, June 18th 2018, amended with *Watchdata GP170003 Detailed Technical Evaluation Report_V10 Annex,* Version 2.0, August 16th 2018.

The evaluation laboratory raised two security recommendations that introduce some limitations on the usage of the TOE, which are included in the [ST] and in the [Dev_guide], namely:

- **R.PROPRIETARY_API,** which recommends using GlobalPlatform API over proprietary APIs and provides the list of the proprietary APIs that must not be used.
- **R.CRYPTO_LIB,** which lists the cryptographic APIs that must not be used. Note: This recommendation is a complement to R.CRYPTO_ALG.

The evaluation laboratory determined that:

- The Security Target [ST] is conformant to the TEE Protection Profile v1.2.1 – Base PP (without “Time & Rollback” and “Debug” PP-Modules);
- The TOE successfully passed the security functional testing and random numbers quality test;
- All the vulnerabilities identified during the source code review and testing campaigns have been corrected or have given rise to security usage recommendations;
- The [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] and [Final_guide] are fulfilled. This includes:

- A.PROTECTION_AFTER_DELIVERY, A.TA_DEVELOPMENT, A.ROLLBACK, A.SOC_PACKAGE, A.TA_MANAGEMENT and A.UUID_MANAGEMENT (see section 2.6);
- R.CRYPTO_ALG (see section 2.5), and R.PROPRIETARY_API, R.CRYPTO_LIB (see section 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 WatchTrust 2.1.1 on SC9860 has been performed as required by the GlobalPlatform 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 WatchTrust 2.1.1 on SC9860 in conformity with the scheme Certification Process [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 and thus requested from the sponsor of the certificate.

5 References

Table 5-1: GlobalPlatform References

Document	Description	Ref
GP_PRO_023	GlobalPlatform TEE Certification Process v1.0	[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	[TEE EM]
GPD_NOT_051	Application of Attack Potential to Trusted Execution Environment v1.4.0 – Confidential	[TEE AP]
GPD_SPE_050	GlobalPlatform Device Technology TEE Common Automated Tests v1.0 As amended by GlobalPlatform TEE Security Test Suite v1.0.2	[TEE CAT]
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	

Table 5-2: Product-related References

Document	Description	Ref
Security Target	TEE(WatchTrust) Security Target, ref. WD_SE_001, version 1.3.3, August 16th 2018 SHA256(Watchdata-Watchtrust-ST-WD_SE_001-1.3.3.pdf) = d05a730596acfba97b352a05ab5074d684089d057fd39355e2fb760a8d2ecad9	[ST]
Guidance	[Integr_guide] WatchTrust Integration Guide for Spreadtrum, ref. WD_WT_001, version 1.1, August 16th 2018 SHA256(WatchTrust-IntegrationManual-for-Spreadtrum-WD_WT_001.pdf) = 3755c920482b90b4fe9f14b3d4e0d652bafbf63d6e884ab6da6a77a37fd123ae	[Integr_guide]
Guidance	[Dev_guide] WatchTrust Developer's Guide, ref. WD_WT_002, version 1.3, August 16th 2018 SHA256(WatchTrust-Develop_Guide-WD_WT_002.pdf) = cf0e0eff63d2f9cd2f8d5f9c7e2cb06a7fb72f7cac8dcc6581c3712a27dc8ff0	[Dev_guide]

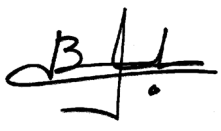
Document	Description	Ref
Guidance	[Final_guide] WatchTrust Final Users Guide, ref. WD_WT_003, version 1.1, August 16th 2018 SHA256(WatchTrust-FinalUsersGuide-WD_WT_003.pdf) = 47ea91edb064975648bbda4f36e818cea514a545f40e1abfdb39ff3f4647c446	[Final_guide]
Evaluation Report	Watchdata GP170003 Detailed Technical Evaluation Report_V10, version 1.0, June 18th 2018 SHA256(Watchdata GP170003 Detailed Technical Evaluation Report_V10.pdf) = fe0d0d01964cff2c11e6a6cae5324835d4a88e167d2ac0bb634bc2ef3991123d amended with Watchdata GP170003 Detailed Technical Evaluation Report_V10 Annex, version 2.0, August 16th 2018 SHA256(Watchdata GP170003 Detailed Technical Evaluation Report_V10-Annex-V20.pdf)= 7fa6db6f46ea8dbf791b6ded830bb882905ab89301902d5da089e86414bbd9e7	[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	
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]

Document	Description	Ref
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



Gil Bernabeu
2018.09.04
12:23:18 +02'00'