GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certificate of Security Evaluation

Huawei iTrustee on Kirin 980 Version 3.0

Certification Number:	GP-TEE-2020/02	**Product Name:**	Huawei iTrustee v3.0 on Kirin 980
Issuance Date:	2020.11.06	**Trusted OS / Developer:**	iTrustee v3.0 / Huawei Technologies Co, Ltd
Sponsor:	Huawei Technologies Co, Ltd.	**SoC / Developer:**	Kirin 980 / Hisilicon
Protection Profile:	TEE PP v1.2.1 – Base PP	**Product Type:**	☐ TEE on Final Device ☑ TEE on SoC ☐ TEE partial scope: ☐ HW/SW ☐ HW ☐ SW
PP-Modules:	None		
Certification Type:	☑ Full ☐ Restricted	**Evaluation Type:**	☑ Full ☐ Delta ☐ Fast-track
Certification Report:	GP-TEE-2020/02-CR	**Security Evaluation Lab:**	Thales ITSEF (Labège, France)

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, Certification Director

GLOBALPLATFORM®
CERTIFIED TEE

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform TEE Security Evaluation Secretariat

Certification Report

GP-TEE-2020/02-CR v1.0

Issue date:	2020.11.06
Product:	Huawei iTrustee v3.0 on Kirin 980
Sponsor:	Huawei Technologies Co, Ltd. Bantian, Longgang District, Shenzhen 518000, P.R.China
Developer(s):	Huawei Technologies Co, Ltd. Hisilicon No. 1599, Xinjinqiao Rd, Pudong Distrinct, Shanghai, 201206, P.R.China Huawei Central Software Building Q27, No. 156 Beiqing Rd, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan, Hai-Dian District, Beijing 100095, P.R.China
Laboratory:	Thales ITSEF 290 allée du Lac, 31670 Labège (France)
Conformance:	TEE PP v1.2.1 (Base PP)
Product Type:	☐ TEE on Final Device ☑ TEE on SoC ☐ TEE partial scope: ☐ HW/SW ☐ HW ☐ SW
Evaluation Type:	☑ Full ☐ Delta ☐ Fast-track
Certification Type:	☑ Full ☐ Restricted On the basis of Common Criteria Certificate ref. ANSSI-CC-2020/67

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 Common Criteria certified product *Huawei iTrustee v3.0 on Kirin 980*, developed by Huawei Technologies Co, Ltd. (Hisilicon and Huawei Central Software), registered under number GP200008.

The evaluation has been performed by Thales ITSEF in Labège (France) under ANSSI supervision. The product has been certified under the reference ANSSI-CC-2020/67.

The present certification has been performed under the GlobalPlatform and ANSSI Memorandum of Understanding dated 1st September 2015.

The following documents constitute the basis for this Certification Report: *Huawei iTrustee v3.0 on Kirin 980 Security Target v1.9* [ST] and the *Certification Report ANSSI-CC-2020/67* [CCCR].

By this Certification Report GlobalPlatform recognises the results of the Common Criteria certification under reference ANSSI-CC-2020/67, which confirms that the security target [ST] is conformant to the *GlobalPlatform TEE Protection Profile v*1.2.1 - *Base PP* [TEE PP] and that the evaluated product *Huawei iTrustee v3.0 on Kirin 980* is consistent with its security target for the evaluation level EAL 2 augmented with AVA_TEE.2. The certificate is valid provided the guidance [AGD_PRE] and [AGD_OPE] is applied.

2 Product information

2.1 Identification

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

Table 2-1: Product identification

Product identification	
Product Name	Huawei iTrustee v3.0 on Kirin 980
Developer	Huawei Technologies Co, Ltd. Hisilicon Huawei Central Software
Product Type	TEE on SoC

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

Table 2-2: TOE components identification

TOE components identification		**Developer**
SoC reference	Kirin 980	Hisilicon
Boot code	Fastboot v1.0 MD5 Hash: 2561c3f407199abcb18633155df398ad	Hisilicon
ATF binary	ATF v1.0 MD5 Hash: b105cc4d51511f4b4290f48e2c782aab	ARM / Hisilicon
TEE binary	iTrustee v3.0 MD5 Hash: 79d5fd6ea04d43134e12dd94218fc612	Huawei Technologies Co, Ltd

2.2 Documentation

The Product documentation consists of the security target and guidance documentation:

- [ST] *Huawei iTrustee v3.0 on Kirin 980 Security Target v1.9*, compliant with *TEE Protection Profile v1.2.1 - Base PP* [TEE PP];
- [AGD_PRE] *Huawei iTrustee V3.0 on Kirin 980 Preparative Procedures for User, version 1.6*;
- [AGD_OPE] *Huawei iTrustee V3.0 on Kirin 980 Operational User Guidance, version 1.2*.

2.3 Architecture

The hardware architecture of the TOE includes: internal RAM, cryptographic accelerators, processing cores, timer, ROM and OTP. The external memories (Flash and DDR) are not part of the TOE.

The firmware and software architecture of the TOE consists of Secure Boot firmware, ATF firmware, iTrustee Kernel, TEE Communication Agent, Trusted Core Framework and Trusted Device Drivers. The REE is not part of the TOE.

The TOE implements the GlobalPlatform API listed in Table 2-3, for which Huawei does not make any functional compliance claim in the security target.

Table 2-3: GlobalPlatform API

Reference		Version
GPD_SPE_010	GlobalPlatform TEE Internal Core API Specification	1.2

2.4 Life-cycle

The TOE life cycle is split in the following development, manufacturing and usage phases.

- Phase 1 corresponds to the firmware, software and hardware design;
- Phase 2 corresponds to the SoC manufacturing;
- Phase 3 corresponds to the software integration;
- Phase 4 corresponds to the device production;
- Phase 5 stands for the end-usage of the device.

The TOE operational phase starts in Phase 4.

2.5 Security Functionality

We refer to the [ST] and [CCCR] for the description of the security functionality in the scope of the evaluation.

The TOE relies on the following cryptographic functionality, which is in the scope of the CC evaluation (FCS_COP.1 requirements):

- RSA 2048 and SHA 256 for the verification of the authenticity of TEE firmware and software;
- RSA 2048 and SHA 256 for the verification of the authenticity of TA code;
- HMAC, AES_XTS_256 and CMAC for protecting the consistency and confidentiality of Trusted Storage data, by using the TEE storage root of trust key.

Table 2-4 presents the cryptographic operations supported by the Product according with the [ST]. However, only those identified in FCS_COP.1 are in the scope of the evaluation.

GlobalPlatform cryptographic algorithms recommendations defined in [CRYPTO] apply.

Table 2-4: List of cryptographic algorithms

Algorithm	Supported modes	Key length (bits)	Supported standards
Symmetric ciphers (AES)	CBC CTS XTS CTR OFB	128, 192, 256, 512 (XTS)	FIPS 197 (AES) NIST SP800-38A (CBC, CTR) IEEE Std 1619-2007 (XTS) NIST SP800-38A Addendum (CTS = CBC-CS3)
Symmetric ciphers (3DES)	CBC	128 or 192	FIPS 46 (DES, 3DES) FIPS 81 (CBC)
Hashing	SHA1 SHA224 SHA256 SHA384 SHA512		FIPS 180-4 (SHA1 SHA224 SHA256 SHA384 SHA512)

Algorithm	**Supported modes**	**Key length (bits)**	**Supported standards**
MAC (HMAC)	SHA1 SHA224 SHA256 SHA384 SHA512	block size not exceed（64bytes for SHA-1 and SHA-224/256, 128bytes for SHA-384/512	RFC 2202 (SHA1) RFC 4231 (SHA224 SHA256 SHA384 SHA512)
MAC(AES_MAC)	AES_MAC CMAC GCM GMAC	128, 256	NIST SP800-38B
Authen EncryModes	AES_CCM	128, 192, 256	RFC 3610 (CCM)
Asymmetric cipher (encrypt/decrypt)	TEE_ALG_RSA_NOPAD TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA1 TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA224 TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA256 TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA384 TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA512 TEE_ALG_RSAES_PKCS1_V1_5	2048, 3072	PKCS #1 (RSA, PKCS1 v1.5, OAEP) FIPS 180-4 (SHA-1, SHA-2)
Asymmetric cipher (sign/verify)	TEE_ALG_RSASSA_PKCS1_V1_5_SHA224 TEE_ALG_RSASSA_PKCS1_V1_5_SHA256 TEE_ALG_RSASSA_PKCS1_V1_5_SHA384 TEE_ALG_RSASSA_PKCS1_V1_5_SHA512 TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA224 TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA256 TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA384 TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA512	2048, 3072	PKCS #1 (RSA, PKCS1 v1.5, PSS) FIPS 180-4 (SHA-2)
Key Derivation	DH	2048	PKCS #3 FIPS 186-4* ANSI X9.62 NIST SP800-56A, Cofactor Static Unified Model FIPS 186-4* (curve definitions)
ECC	ECDSA ECDH	160, 192, 224, 256, 384 and 521	FIPS 186-4* ANSI X9.62

2.6 Objectives for the environment

The *Huawei iTrustee v3.0 on Kirin 980 Security Target v1.9* [ST] defines the following objectives for the environment conformant with the *TEE Protecton Profile* [TEE PP].

Note that

- The [ST] adds some complementary information to OE.INTEGRATION_CONFIGURATION and OE.TA_DEVELOPMENT.
- A refinement OE.EXT_MEM for the protection of DDR applies to OE.INTEGRATION_CONFIGURATION.

OE.INTEGRATION_CONFIGURATION

Integration and configuration of the TEE by the device manufacturer shall rely on guidelines defined by the TOE 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.

Complementary information: The TOE shall be installed and configured correct to ensure the TOE running in a secure state. The process of TEE identifier generating shall ensure statistical uniqueness of the TEE identifier.

OE.EXT_MEM: The CPU and DDR shall be integrated in a PoP package.

OE.PROTECTION_AFTER_DELIVERY

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.

OE.ROLLBACK

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.

OE.SECRETS

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

OE.TA_DEVELOPMENT

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

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

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

Complementary information: TA developers should apply for TA identifiers from the TOE manufacturer before deploying the TA into the TOE. All of the TA identifiers are generated, issued and managed by the TOE manufacturer.

2.7 Clarification of Scope

The TOE does not include any pre-loaded Trusted Application.

The REE and the external Flash and DDR memories are out of the evaluation scope (see. [CCCR]). However, the TOE ensures the protection of the data stored in Flash through the Trusted Storage security functionality, and DDR and CPU are expected to be integrated in a PoP package as stated in OE.EXT_MEM (see section 2.6).

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

Development and manufacturing sites as well as the procedures applicable in Phases 1 to 3 are out of the scope of the evaluation.

3 Evaluation

3.1 Evaluation Laboratory Identification

The evaluation has been performed by Thales ITSEF, located 290 allée du Lac, 31670 Labège (France), accredited by GlobalPlatform under reference GP_AL_018.

3.2 Evaluated Configuration

The evaluation addressed the TOE identified in section 2.1. Any deviation from the indicated components brings the TOE outside the evaluated configuration.

3.3 Evaluation Activities

The evaluation has been performed under ANSSI supervision in compliance with Common Criteria v3.1 R5 [CC], Common Evaluation Methodology v3.1 R5 [CEM] and AVA_TEE.2 as defined in [TEE PP].

The generation of random numbers was analyzed following [NIST SP 800-90A]; no vulnerability was found for the level AVA_TEE.2.

We refer to [CCCR] for more information.

3.4 Evaluation Results

The certification report [CCCR] confirms the following:

- The *Huawei iTrustee v3.0 on Kirin 980 Security Target v1.9* [ST] is conformant to the *GlobalPlatform TEE Protection Profile v1.2.1 - Base PP* [TEE PP];
- The Product *Huawei iTrustee v3.0 on Kirin 980* is consistent with its security target for the evaluation level EAL 2 augmented with AVA_TEE.2;
- The certificate *ANSSI-CC-2020/67* is valid provided the guidance [AGD_PRE] and [AGD_OPE] is applied.

4 Certification

4.1 Usage Restrictions

The user of the certified product must ensure that the objectives for the environment (see section 2.6) defined in the security target [ST], the guidance [AGD_PRE] and [AGD_OPE] and the following GlobalPlatform recommendations are applied:

- Recommendation on the protection of the external DDR as defined in OE.EXT_MEM (see section 2.6);
- Cryptographic algorithms recommendations defined in [CRYPTO].

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 there is sufficient evidence to affirm that the product *Huawei iTrustee v3.0 on Kirin 980* meets its security target [ST] and the requirements of AVA_TEE.2, provided all the usage restrictions defined in section 4.1 are fulfilled.

GlobalPlatform issues the Full Certificate for *Huawei iTrustee v3.0 on Kirin 980* by recognition of ANSSI-CC-2020/67 certificate in accordance with the *GlobalPaltform TEE Certification Process* [TEE CP] and within the framework of the GlobalPlatform and ANSSI MOU dated Sept 1st 2015.

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

5 References

Table 5-1: GlobalPlatform References

Document	Description	Ref
GP_PRO_023	GlobalPlatform TEE Certification Process v1.0	[TEE CP]
GPD_SPE_021	GlobalPlatform Device Committee TEE Protection Profile v1.2.1	[TEE PP]
GPD_NOT_051	Application of Attack Potential to Trusted Execution Environment v15.0.11– Confidential	[TEE AP]
GP_TEN_053	GlobalPlatform Technology Cryptographic Algorithm Recommendations v1.0	[CRYPTO]
GPD_SPE_010	TEE Internal Core API Specification v1.2	[IAPI]

Table 5-2: Common Criteria References

Document	Description	Ref
Common Criteria	Common Criteria for Information Technology Security Evaluation: - Part 1: Introduction and general model, avril 2017, version 3.1, revision 5, reference CCMB-2017-04-001 - Part 2: Security functional components, avril 2017, version 3.1, revision 5, reference CCMB-2017-04-002 - Part 3: Security assurance components, avril 2017, version 3.1, revision 5, reference CCMB-2017-04-003	[CC]
Common Evaluation Methodology	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, avril 2017, version 3.1, revision 5, reference CCMB-2017-04-004	[CEM]

Table 5-3: Product References

Document	Description	Ref
Security Target	Huawei iTrustee v3.0 on Kirin 980 Security Target v1.9	[ST]
Guidance	Huawei iTrustee V3.0 on Kirin 980 Preparative Procedures for User, version 1.6, 29/04/2019	[AGD_PRE]
Guidance	Huawei iTrustee V3.0 on Kirin 980 Operational User Guidance, version 1.2, 16/03/2019	[AGD_OPE]
Common Criteria Certification Report	Rapport de certification ANSSI-CC-2020/67 - iTrustee on Kirin 980 (Version 3.0). July 2020	[CCCR]

Table 5-4: External References

Document	Description	Ref
NIST Special Publication	Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A. January 2012	[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]
NIST Special Publication	NIST SP800-38A - Recommendation for Block Cipher Modes of Operation, October 2010	
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]
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]
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
CC	Common Criteria
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
HMAC	(keyed-)Hash Message Authentication Code
MAC	Message Authentication Code
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

Mounji Methlouthi

Signature numérique de Mounji Methlouthi
DN : c=US, st=California, l=Redwood City, o=GlobalPlatform, Inc., cn=Mounji Methlouthi, email=mounji.methlouthi@smart-consulting.com
Date : 2020.11.08 07:17:32 +01'00'