Reference: 2019-52-INF-3892- v1
Target: Limitada al expediente
Date: 21.09.2022

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-52**
TOE	**Huawei SUN2000HA Software V300R001C00SPC608**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**

References

[EXT-5510] Certification Request

[EXT-7889] Evaluation Technical Report

Certification report of the product Huawei SUN2000HA Software V300R001C00SPC608, as requested in [EXT-5510] dated 10/10/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7889] received on 15/07/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei SUN2000HA Software V300R001C00SPC608.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: No.

Evaluation Level: Common Criteria v.3.1 R5 - EAL3 + ALC_FLR.2.

Evaluation end date: 22/07/2022.

Expiration Date[1]: 20/09/2027

All the assurance components required by the evaluation level EAL3 (augmented with ALC_FLR.2 Flaw reporting procedures) have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 + ALC_FLR.2, as defined by the Common Criteria v.3.1 R5 and the Common Methodology for Information Technology Evaluation v.3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei SUN2000HA Software V300R001C00SPC608, a positive resolution is proposed.

TOE SUMMARY

The TOE is the software running in the Operating System that is deployed into communication board inside Huawei SUN2000HA inverter, which is the access node of inverter. The TOE is a 'software only'. TOE consists of the software running on the Operating System of the SUN2000HA inverter chassis, but not the hardware.

The TOE provides near-end maintenance through:

- Huawei mobile phone APP connected to the SUN2000HA inverter through the USB-WIFI Adapter stick inserted into the USB terminal.
- Smartlogger connected to the SUN2000HA inverter through the MBUS or RS485 with Modbus-RTU protocol (in the TOE evaluated configuration is used the RS485 port).

The TOE provides the following major security features:

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

- Authentication and Authorization: Only authenticated users are allowed to log in to the TOE, query TOE data, and set TOE parameters. Only authorized users are able to execute the previous actions based on their privileges. If a user fails to be authenticated for multiple consecutive times, the user is locked for a period of time to prevent unauthorized access.
- Auditing: An operation log records the operation that an administrator has performed on the system and the result of the operation and is used for tracing and auditing.
- Security Management: The TOE provides four different user roles (Common user, Advanced user, Special user and Datalogger user). Also, the TOE provides: user password management, software upgrade, log exports and time settings.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 and the evidences required by the additional component ALC_FLR.2 Flaw reporting procedures according to Common Criteria v3.1 R5.

Assurance class	Assurance components
ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1
ADV	ADV_ARC.1 ADV_FSP.3 ADV_TDS.2
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.3 ALC_CMS.3 ALC_DEL.1 ALC_DVS.1 ALC_LCD.1 ALC_FLR.2
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the functional requirements according to the Common Criteria v3.1 R5 declared in section 6 Security Requirements of the TOE in the Security Target.

IDENTIFICATION

Product: Huawei SUN2000HA Software V300R001C00SPC608

Security Target: CC Huawei SUN2000HA Software V300R001C00SPC608 Security Target, version 1.6, 2022-05-11.

Protection Profile: No.

Evaluation Level: Common Criteria v.3.1 R5 - EAL3 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Huawei SUN2000HA Software V300R001C00SPC608 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.4 Organizational Security Policy.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions documented in the Security Target section 3.5 Assumptions, are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats documented in the Security Target section 3.3 Threats, do not suppose a risk for the product Huawei SUN2000HA Software V300R001C00SPC608, although the agents implementing attacks have a *Basic* attack potential according to Common Criteria v.3.1 R5 EAL3 + ALC_FLR.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 Security Objectives for the operational Environment.

ARCHITECTURE

LOGICAL ARCHITECTURE

All the software run in the communication and control circuit board. Which is responsible communication, managing and controlling, and security features in SUN2000HA inverter. In terms of the software, SUN2000HA software architecture consists of three logical planes to support centralized controlling and management and running status sampling.

- Plugin plane
- Core plane
- Sampling and Controlling plane

The plugin plane provides external communication services and near-end maintenance services. Processes protocols and signals, configures and maintains the system status, and reports and controls the system status.

The core plane is the core of the entire system. It provides user management, alarm management, log management, and software upgrade management, etc.

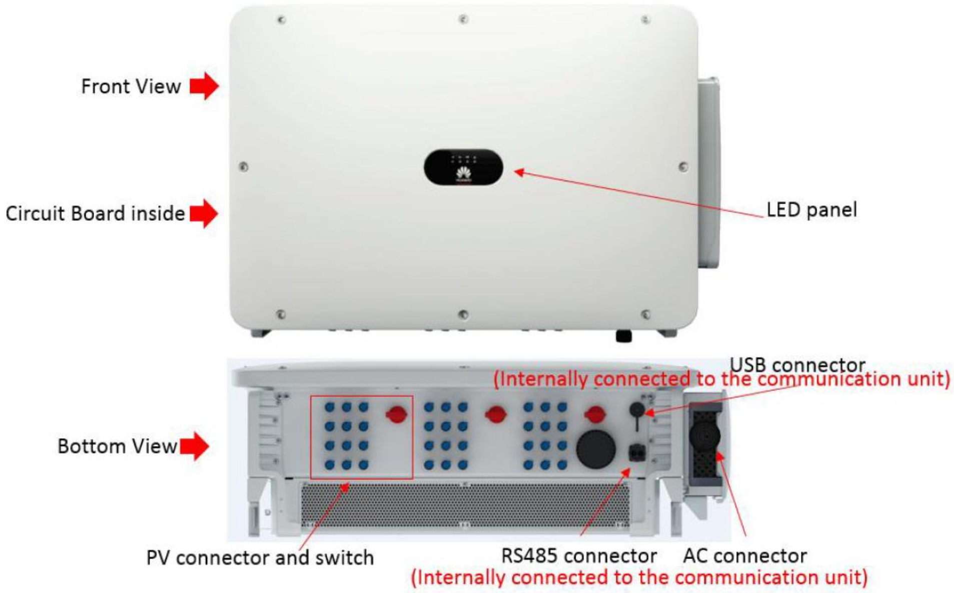
The sampling and controlling plane is used to manage system and sample data.

PHYSICAL ARCHITECTURE

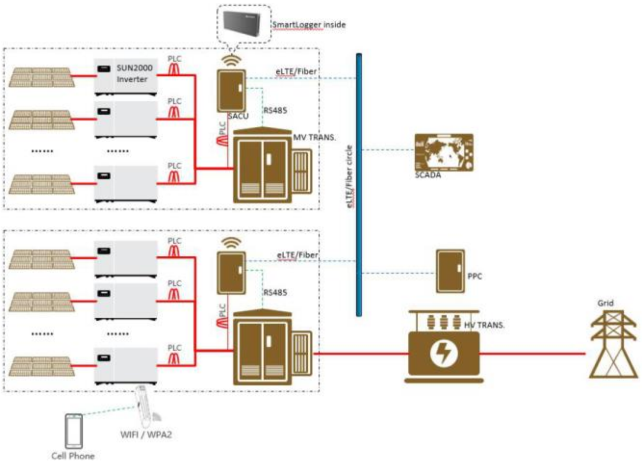
The product SUN2000HA inverter consists of the hardware and the software. The TOE is the software running in the Operating System that is deployed into communication board inside Huawei SUN2000HA inverter, which is the access node of inverter. The TOE is a 'software only'

The hardware is composed of chassis, circuit boards, LED panel and connectors. The chassis is used to install circuit boards, including power circuit boards and communication boards. The LED panel is used to indicate the operating status of the system. The connectors is used to connect to PV plant, AC Grid, USB-WiFI Adapter stick and USB disk.

The USB terminal and AC terminal are internally connected to the communication unit.



The main service provided by this inverter is to convert the direct current of photovoltaic panels into alternating current that can be feed-in to the grid. The PV terminals are used to connect photovoltaic panels. The AC terminal is used to connect to the grid.

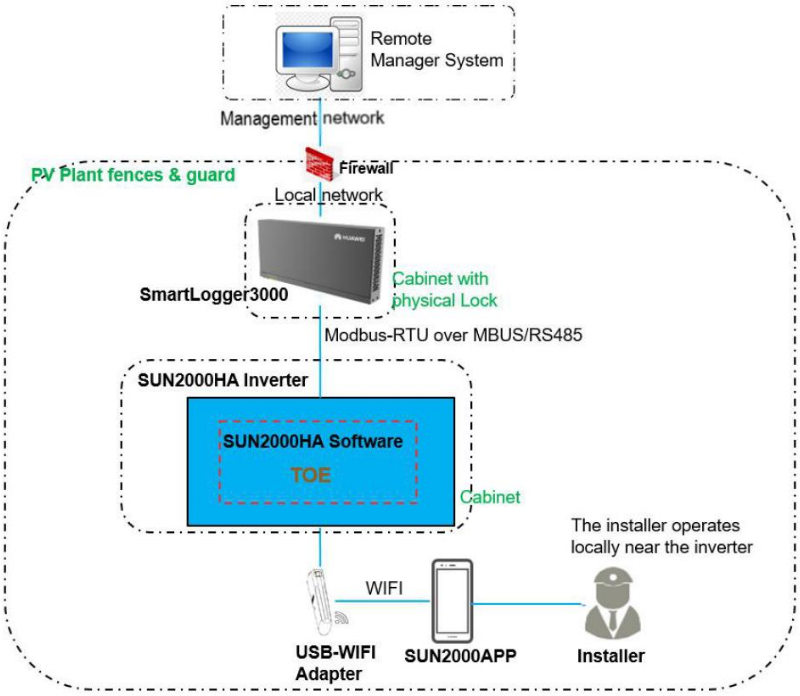


The environment for TOE comprises the following components:

Non-TOE	Item or module type	Requirement
Mobile phone	Huawei Mobile phone	Operating system: android 4.4 or later

Mobile phone app	SUN2000APP	Software version: 3.2.00.016
USB-WIFI Adapter stick	USB-Adapter2000-C	
Remote Manager System PC	Desktop PC	Supported web browsers: Firefox52, Chrome 58 and IE9 or above
Security Firewall	Firewall	
SmartLogger	SmartLogger3000	Software version:V300R001C00SPC605 or greater
SUN2000HA inverter	SUN2000HA 185KTL-H1	Note: SUN2000HA 185KTL-H1, SUN2000HA 175KTL-H0 and SUN2000HA 185KTL-INH0 are the same series inverter.

The TOE in its operational environment is depicted below:



DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

Delivery Item	Version	Format	SHA256
SUN2000-(175KTL-H0, 185KTL-INH0, 185KTL-H1) Series User Manual	13	pdf	1a700bd3d2f279960414e 861d2f5f1b0 a8335cf3e0f471a24ba0e6175d05b90c
FusionSolar App and SUN2000 App User Manual	02	pdf	09190b4b27db2ee653863d5dc49c3b 3f8283e6f27aeea7a6e30d6915e37dbd58
CC Huawei SUN2000HA Software V300R001C00SPC608 AGD_OPE	1.1	pdf	1f740fafd3155714ae0e29ca6768787 82219886f8db3ca0c9c6f3bf0352b309d
CC Huawei SUN2000HA Software V300R001C00SPC608 AGD_PRE	1.1	pdf	6acc9312d0d92fef359c9b9ba1931d3 517a92bc52f3a86dc55232c8c081d4301
SUN2000-(175KTL-H0, 185KTL-INH0, 185KTL-H1) MODBUS Interface Definitions	0.3	pdf	a4a26a0535d4f11f3c3cff9d818f94f78 64d3f22a426c225ac87e6722b9bad14
SUN2000HA V300R001C00 Communication Matrix	02	xls	28c28057f9d678e702cc2a9fb969b3ee c8f50a800b5c2b4c1d81a5da23747302

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated all of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The TOE Huawei SUN2000HA Software V300R001C00SPC608 is a 'software only'. TOE consists of the software running on the Operating System of the SUN2000HA inverter chassis, but not the hardware.

The software in the delivered product is pre-burned on the factory production state using an old version, therefore, the final user shall update the product to the TOE with the software defined in the table below to reach the evaluated version.

Type	Delivery Item	Version	Format	SHA256
Software	SUN2000HAV300R001C00SPC608_package.zip	V300R001C00SPC608	.zip	74ccda90f7a5632a5441119da9ee5a99f341d220c6fac92eabcee87b925f8be5
Software Signature File	SUN2000HAV300R001C00SPC608_package.zip.asc	-	.asc	NA

The TOE Huawei SUN2000HA Software V300R001C00SPC608, the signature file and the associated documentation can be downloaded from the Huawei's support website:

> https://support.huawei.com/enterprise/en/digital-power/sun2000ha-pid-21785801/software/254406651?idAbsPath=fixnode01%7C9452479%7C21439560%7C7921563%7C21102414%7C21785801

To download the software, you need to have a Huawei account of the support website first, and please register an account role with download permission.

EVALUATION RESULTS

The product Huawei SUN2000HA Software V300R001C00SPC608 has been evaluated against the Security Target CC Huawei SUN2000HA Software V300R001C00SPC608 Security Target, version 1.6, 2022-05-11.

All the assurance components required by the evaluation level EAL3 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3 + ALC_FLR.2, as defined by the Common Criteria v.3.1 R5 and the Common Methodology for Information Technology Evaluation v.3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product:

The TOE usage is recommended given that there are not exploitable vulnerabilities for the TOE under its operational environment. The following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.
- The fulfillment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei SUN2000HA Software V300R001C00SPC608, a positive resolution is proposed.

The certifier recommends to TOE consumers to strictly follow the recommendations from the evaluation team listed above.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- CC Huawei SUN2000HA Software V300R001C00SPC608 Security Target, version 1.6, 2022-05-11.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.