Reference: 2019-19-INF-3679- v1
Target: Pública
Date: 02.02.2022

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-19**
TOE	**Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-4929] Certification request

[EXT-7321] Evaluation technical report

Certification report of the product Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004, as requested in [EXT-4929] dated 23/04/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7321] received on 30/07/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004.

Huawei Reliable Telecomm OS is a highly-configurable Linux-based operating system for embedded devices, which has been developed to provide a good level of security as required in commercial environments.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

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

Protection Profile:

- Operating System Protection Profile, BSI-CC-PP-0067, Version 2.0; strict conformance;
- OSPP Extended Package - Advanced Management, BSI-CC-PP-0067, OSPP EP-AM, Version 2.0; strict conformance

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1 R5 - EAL4+ (ALC_FLR.3).

Evaluation end date: 18/11/2021

Expiration Date[1]: 01/02/2027

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.3) 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 EAL4, as defined by the Common Criteria for Information Technology Security Evaluation Version 3.1 R5 and the Common Methodology for Information Technology Security Evaluation Version 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004, a positive resolution is proposed.

[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.

TOE SUMMARY

Huawei Reliable Telecomm OS is a general purpose, multi-user, multi-tasking Linux based operating system for embedded devices.

The following hardware are fully compatible with TOE:

- ARM64 based device board (using ARM64 v8 processor) with Huawei hi1382: 16-core ARM cortex-A72, 1GB flash storage, serial port and network port interface, with external 48v DC power module.
- ARM64 based device board (using ARM64 v8 processor) with Huawei hi1213: 4-core ARM cortex-A72, LowPower dissipation, 8GB ram, 1GB flash storage, serial port and network port interface, with external 48v DC power module.

All ARM64 device board using ARM64 v8 processors supports TOE running.

Additionally, the TOE needs an OS Linux x86_64 machine for administration.

The TOE provides the following key security features:

- Security Audit: The TOE is able to intercept all system calls and recording the events occurred in the system. The security audit functionality also allows to configure the events to be audited, review and search the audit log retrieved.
- Cryptographic support: The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. It is achieved by using the SSHv2 protocol. The TOE also provided TLS protocols in order to secure the communications with other IT entities.
- Identification and Authentication: The TOE includes several ways to identify and authenticate the users (via the local console using username and password or via the SSH using password and public-key based authentication. The TOE also offers a password quality enforcement mechanism as well as it is able to handle failed authentication attempts.
- User Data Protection: The TOE offers a Discretionary Access Control (DAC) which allow owner of named objects to control the access permissions to these objects. Moreover, the TOE kernel implements the IPTables mechanism in order to provide a packet filter at network and transfer layer. Using these two mechanism the TOE offers an access control policy as well as an information flow control policy.
- Security Management: The TOE offers to the users and/or authorized administrators the possibility of modify the configuration of TSF. The TOE allows local and remote management using by using OpenSSH.
- TOE Access: The TOE is able to end user sessions after an inactivity period of time. This can be initiated by the TSF itself or by user request.
- Trusted Channel: Using the cryptographic communication protocols above mentioned (SSH and TLS) the TOE is able to establish secure and trusted communication channel with other IT entities.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_FLR.3 to the table, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
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.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.3
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.3

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria for Information Technology Security Evaluation Version 3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS	
FAU_GEN.1 Audit data generation 31	FAU_GEN.2 User identity association 32
FAU_SAR.1 Audit review 32	FAU_SAR.2 Restricted audit review 32
FAU_SEL.1 Selective audit 32	FAU_STG.1 Protected audit trail storage 33
FAU_STG.3 Action in case of possible audit data loss 33	FAU_STG.4 Prevention of audit data loss 33
FCS_CKM.1 (SYM) Cryptographic key generation 34	FCS_CKM.1 (RSA) Cryptographic key generation 34
FCS_CKM.1 (DSA) Cryptographic key generation 35	FCS_CKM.1 (ECDSA) Cryptographic key generation 35
FCS_CKM.2 (NET) Cryptographic key distribution 35	FCS_CKM.4 Cryptographic key destruction 36

FCS_COP.1 (NET) Cryptographic operation 36	FCS_RNG.1 Random number generation (Class DRG.2) 37
FDP_ACC.1 (PSO) Subset access control 38	FDP_ACC.1 (TSO) Subset access control 38
FDP_ACF.1 (PSO) Security attribute based access control 39	FDP_ACF.1 (TSO) Security attribute based access control 40
FDP_IFC.2 (NI) Complete information flow control 41	FDP_IFF.1 (NI) Simple security attributes 41
FDP_ITC.2 Import of user data with security attributes 43	FDP_RIP.2 Full residual information protection 43
FDP_RIP.3 Full residual information protection of resources 44	FIA_AFL.1 Authentication failure handling 44
FIA_ATD.1 (HU) User attribute definition 44	FIA_ATD.1 (TU) User attribute definition 45
FIA_SOS.1 Verification of secrets 45	FIA_UAU.1 Timing of authentication 45
FIA_UAU.5 Multiple authentication mechanisms 45	FIA_UAU.7 Protected authentication feedback 46
FIA_UID.1 Timing of identification 46	FIA_USB.2 Enhanced user-subject binding 46
FMT_MSA.1 (PSO) Management of object security attributes 48	FMT_MSA.1 (TSO) Management of object security attributes 48
FMT_MSA.3 (PSO) Static attribute initialization 48	FMT_MSA.3 (TSO) Static attribute initialization 49
FMT_MSA.3 (NI) Static attribute initialization 49	FMT_MSA.4 (PSO) Security attribute value inheritance 49
FMT_MTD.1 (AE) Management of TSF data 50	FMT_MTD.1 (AS) Management of TSF data 50
FMT_MTD.1 (AT) Management of TSF data 50	FMT_MTD.1 (AF) Management of TSF data 50
FMT_MTD.1 (NI) Management of TSF data 50	FMT_MTD.1 (IAT) Management of TSF data 51
FMT_MTD.1 (IAF) Management of TSF data 51	FMT_MTD.1 (IAU) Management of TSF data 51
FMT_MTD.1 (AM-AP) Management of TSF data 51	FMT_MTD.1 (AM-MR) Management of TSF data 51
FMT_MTD.1 (AM-MD) Management of TSF data 52	FMT_MTD.1 (AM-MA) Management of TSF data 52
FMT_REV.1 (OBJ) Revocation 52	FMT_REV.1 (USR) Revocation 52
FMT_SMF.1 Specification of Management Functions 52	FMT_SMR.1 Security roles 53
FPT_STM.1 Reliable time stamps 53	FPT_TDC.1 Inter-TSF basic TSF data consistency 53
FTA_SSL.1 TSF-initiated session locking 53	FTA_SSL.2 User-initiated locking 54
FTP_ITC.1 Inter-TSF trusted channel	

EXTENDED SECURITY FUNCTIONAL REQUIREMENTS
FCS_RNG Generation of random numbers
FDP_RIP.3 Full residual information protection of resources
FIA_USB.2 Enhanced user-subject binding

IDENTIFICATION

Product: Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004

Security Target: Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004 Security Target (version: 1.2, date: 21/07/2021).

Protection Profile:

- Operating System Protection Profile, BSI-CC-PP-0067, Version 2.0; strict conformance;

- OSPP Extended Package - Advanced Management, BSI-CC-PP-0067, OSPP EP-AM, Version 2.0; strict conformance

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1 R5 EAL4 + ALC_FLR.3.

SECURITY POLICIES

The use of the product Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004 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 3.2 ("Organizational Security Policies").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following 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.

The detail of these assumptions is documented in the Security Target, section 3.3 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004, although the agents implementing attacks have the attack potential according to the enhanced-basic attack potential of EAL4 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.

The threats covered by the security properties of the TOE are those defined in the Database Management Systems Protection Profile and they are documented in the Security Target, section 3.1 ("Threats").

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

The TOE contains several subsystems; each of them has several modules and provides some security functionality for other subsystems. The figure below shows these subsystems and the interactions among them.

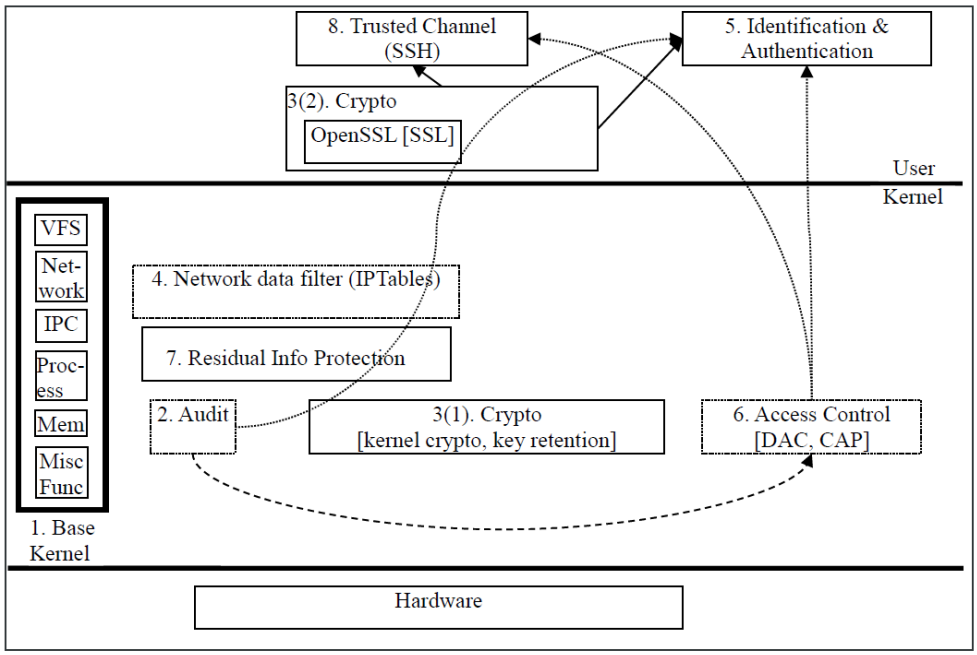

Figure 1. TOE subsystems and interactions among them

Some notes on Figure 1:

- The Base Kernel subsystem is the basis of the whole system; it supports all other subsystems, and provides plenty of APIs for them.

  To make the figure neat, the interaction between the Base Kernel and related subsystems is not shown. Instead, the box for the Base Kernel is widened evidently to indicate this.

- Subsystem Crypto contains two independent parts, one in kernel space and the other in user space, each containing some modules. These parts are denoted with separate boxes in the figure.

- The subsystems denoted with dotted boxes in kernel space are not fully implemented in kernel space. Each of such subsystems contains a group of management facilities that run in user space. To make it easy to understand, these facilities are not shown in the figure.

The table below gives basic information of each subsystem:

No.	Subsystem ID	Subsystem Name	Description
1	S_KNL	Base kernel	Fundamental OS services provided in kernel space, including virtual file system, network protocol stack, inter-process communication mechanisms, process scheduling, memory management, timer/clock and so on.
2	S_AUDIT	Audit	Selection of auditable events, generation of audit records, protection of configurations and audit tracks, tools to review and search audit tracks.
3	S_CRYPTO	Crypto services	Facilities for data randomization, hashing, encryption/decryption and signing/verifying.
4	S_NETCTL	Network data flow filter and control	Rules for network packet filtering and enforcement of the rules.
5	S_IA	User identification and authentication	Management of user identification, local and remote authentication, protection of authentication information, log of failed authentication.
6	S_ACTL	Access control	Traditional Unix discretionary access control capabilities.
7	S_RIP	Protection of residual infomation	Management of information in reusable resources (RAM, disk, IPC).
8	S_TCHNL	Trusted channel	Creation and management of trusted channel between two connected entities, including authentication, key exchange, and session management.

Table 1. TOE subsystems

PHYSICAL ARCHITECTURE

The TOE consists of RPM packages and documentation. These packages and files are provided via email.

- rtos_base-207.3.5.SPC100.B004-20210331120602.i586.rpm

  (sha256: d7f59d8a783705006e0d128c4a6b2e328d2efa52e2c9efe04f6438f264b08144)

- rtos_kernelspace_sysroots-arm64le_4.4_ek_preempt-207.3.5.SPC100.B004-20210331120602.i586.rpm

  (sha256: a65c7e9fc7522cdc72697c8c71856cdfe2d9b723662177c574e48ec8487b1187)

- rtos_libc_sysroots-arm64le_4.4_ek_preempt-207.3.5.SPC100.B004-20210331120602.i586.rpm

  (sha256: 5c89f221574c11a8ea098fc14ba21eaf4a85863856ca8882b6f5eb955cfeb65c)

- rtos_userspace_sysroots-arm64le_4.4_ek_preempt-207.3.5.SPC100.B004-20210331120602.i586.rpm

  (sha256: 5431f3fc0b85fce2d300418189a8943fc38fa51ed905965fab00480d38f0eddd)

- rtos_dist-arm64le_4.4_ek_preempt-207.3.5.SPC100.B004-20210331120602.i586.rpm

  (sha256: cc26f3ce53c06d4b23455b6abc8587f568ce53a7792c61423378914dd5c7f558)

DOCUMENTS

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

- Installation guide: Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004_AGD_PRE-v1.0, delivered in .pdf format

  (sha256: 680f26996a87201994585790f466e3701c230b141c7bbed2b6a8774d00dd9933).

- User guide: Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004_AGD_OPE-v1.0, delivered in .pdf format.

  (sha256: e17102c9208ea177728c08651be14e2414c4e333e055feffe30848b0186fcd69)

- Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004_AGD_OPE_manpage-v1.0, delivered in .tar.gz format: the usage of all the interfaces provided by the TOE.

  (sha256: 94d331aa2c9ba660cf97d25263bbabe9b9348d0483e6af4a70af5bff96e513a3)

- Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004_AGD_PRE_build_tools-v1.0, delivered in .tar.gz format: the usage of helping build the TOE.

  (sha256: 62efcb45115921c5da984b905d3a82651f4235cab5253905c3c78ab533d8dbe5)

PRODUCT TESTING

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

The evaluator designed a set of tests following a suitable strategy for the TOE type taking into account:

1. All SFRs have been tested whether through TSFI excitation or subsystem checking.
2. The testing criteria of the only accessible TSFI is based on:
   - Developer tests rigor.
   - Developer test results including the Web interface and subsystems which tests results are not reliable.
   - Importance of the only accessible TSFI and subsystems.
   - Types of subsystems.
   - Number of subsystems.

In order to create adequate tests, the evaluator has chosen the following criteria: search for critical SFRs and parameters in the TSFI and subsystems, requirements implemented by the only accessible TSFI, exhaustive tests over it and subsystems, incorrect behaviour suspicion with specific input values and the performance of testing every subsystem.

Moreover, the evaluator has carried out tests with the instructions provided for the only accessible TSFI and all subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed the independent test cases including all the security requirements defined in [ST].

The evaluator testing plan has been SFR oriented, and the functionality of each SFR included at the security target has been considered.

All the test cases have been performed using the connection between the local client machine and the Web Interface. This allow testing appropriately both the SFRs defined in [ST] and the subsystems.

This sampling selection was used for the TOE version 207.3.5.SPC100.B004 and covered the 100% of the requirements listed in [ST], the subsystems listed in **Table 1. TOE subsystems** and the TSF-relevant TSFIs.

The test cases have taken into account critical parameters values, searching that the TOE behaves in a non expected manner.

PENETRATION TESTING

The developer has executed a set of penetration tests to check if the potential vulnerabilities may be exploited in the TOE operational environment. The penetration tests have been performed with the assumption that the potential attack is enhanced-basic.

The results obtained when executing the penetration tests demonstrates that the TOE does not present exploited vulnerabilities in the operational environment defined in [ST].

EVALUATED CONFIGURATION

The TOE was tested on the following physical platform:

- ARM64 based device board (using ARM64 v8 processor), Huawei hi1213 Soc based hardware device board (8GB ram, 1GB flash storage, serial port and network port interface, with external 48v DC power module).

The host machine used to connect to the TOE for the evaluation was an OS Linux based machine using Suse Linux 12.4 x86_64.

The evaluated configuration is defined as follows:

- The package set evaluated by CC for the TOE must be selected at install time according to the installation guide and be installed accordingly.
- The TOE supports the use of IPv4 and IPv6, both are also supported in the evaluated configuration.
- The default configuration for identification and authentication include both the defined password-based PAM modules and the key-based authentication for OpenSSH. Support for

other authentication options, e.g. smart card authentication, is not included in the evaluation configuration.

- If the system console is used, it must be connected directly to the TOE and afforded the same physical protection as the TOE.

Configurations and settings that are different from that specified in the installation guide are not permitted.

EVALUATION RESULTS

The product Huawei Reliable Telecomm Operating System version 207.3.5.SPC100.B004 has been evaluated against the Security Target Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004 Security Target (version: 1.2, date: 21/07/2021).

All the assurance components required by the evaluation level EAL4 + ALC_FLR.3 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 EAL4, as defined by the Common Criteria for Information Technology Security Evaluation Version 3.1 R5 and the Common Methodology for Information Technology Security Evaluation Version 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 by the evaluation team given that there are not exploitable vulnerabilities for the TOE under its operational environment. The following usage recommendations are given:

- The fulfilment 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. The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product DEKRA Testing and Certification S.A.U., a positive resolution is proposed.

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.

[OSPP] Operating System Protection Profile, BSI-CC-PP-0067, Version 2.0; strict conformance; https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0067.html

[OSPP-AM] OSPP Extended Package - Advanced Management, BSI-CC-PP-0067, Version 2.0; strict conformance; https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0067.html

[ST] Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004 Security Target (version: 1.2, date: 21/07/2021)

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Huawei Reliable Telecomm Operating System 207.3.5.SPC100.B004 Security Target (version: 1.2, date: 21/07/2021).

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.org.

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.