Reference: 2019-20-INF-3379-v1
Target: Público
Date: 03.02.2021

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

CERTIFICATION REPORT

Dossier #	**2019-20**
TOE	**Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-4930] Certification request

[EXT-6313] Evaluation technical report

Certification report of the product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647, as requested in [EXT-4930] dated 08/05/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-6313] received on 28/10/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647.

The GaussDB 100 is a software-only TOE. GaussDB 100 is a relational database management system (RDBMS) from Huawei Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through structured query language (SQL). GaussDB 100 is a database architecture typically used by global enterprises to manage and process data across wide and local area networks.

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: Protection Profile for Database Management Systems (Base Package), Version 2.12, 23/03/2017 (BSI-CC-PP-0088-V2).

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5 – EAL2 + ALC_FLR.2

Evaluation end date: 25/11/2020

Expiration Date[1]: 03/01/2026

All the assurance components required by the evaluation level EAL2 (augmented with 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 EAL2 + ALC_FLR.2, 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.

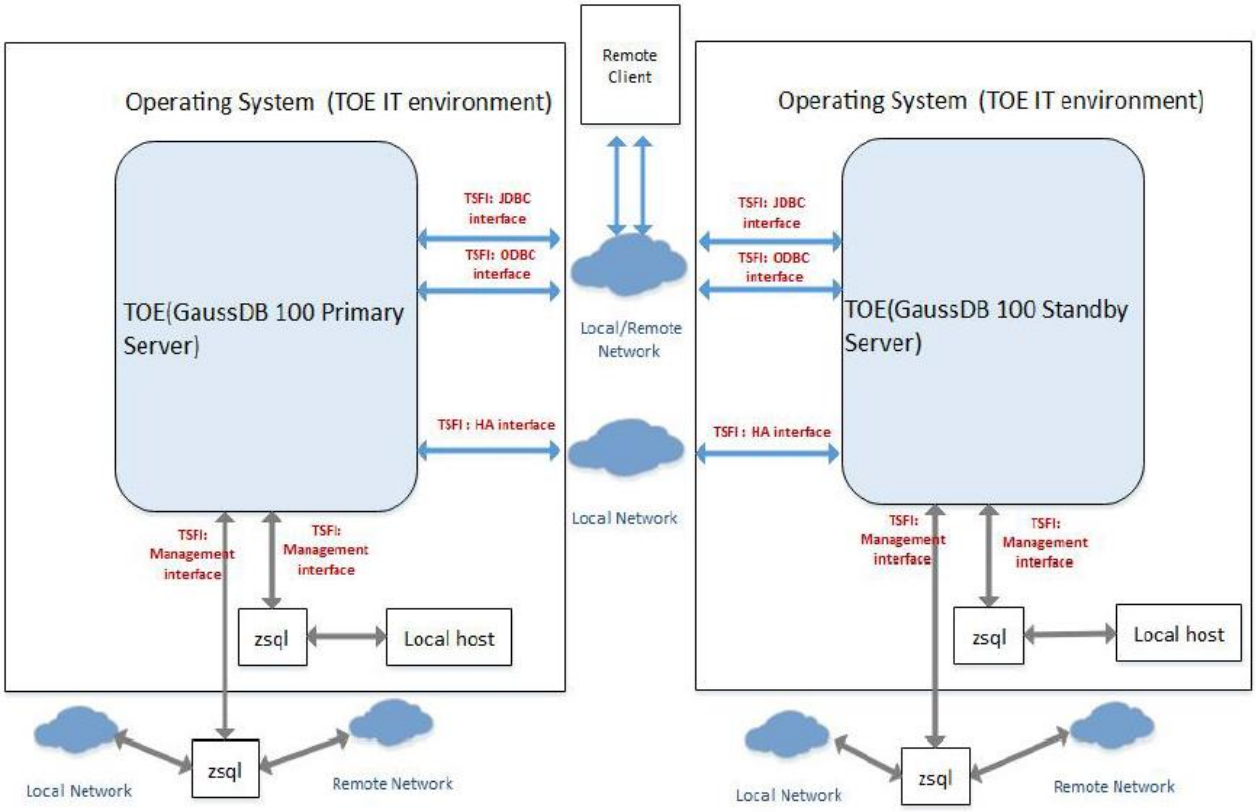
Considering the obtained evidences during the instruction of the certification request of the product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647, a positive resolution is proposed.

[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

The GaussDB 100 is a software-only TOE. GaussDB 100 is a relational database management system (RDBMS) from Huawei Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through structured query language (SQL). GaussDB 100 is a database architecture typically used by global enterprises to manage and process data across wide and local area networks.

Although Huawei GaussDB 100 V300R001C00B300 Release 3da6647 supports two physical deployment modes, client/database configuration and primary/standby database configuration, the evaluated configuration has been the primary/standby database configuration, which is the one covered by this certification.



SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria for Information Technology Security Evaluation Version 3.1 R5.

ASE: Security Target Evaluation	ASE_CCL.1. Conformance claims
	ASE_ECD.1. Extended component definition

	ASE_INT.1. ST Introduction
	ASE_OBJ.2. Security objectives
	ASE_REQ.2. Derived security requirements
	ASE_SPD.1. Security problem definition
	ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture
	ADV_FSP.2. Functional specification
	ADV_TDS.1. TOE design
AGC: Guidance documents	AGD_OPE.1. Operational user guidance
	AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities
	ALC_CMS.2. CM Scope
	ALC_DEL.1. Delivery
	ALC_FLR.2. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage
	ATE_FUN.1. Functional tests
	ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Part 2 of Common Criteria for Information Technology Security Evaluation Version 3.1 R5 and extended components defined in section 6 of the Security Target:

FAU: Security Audit	FAU_GEN.1. Audit data generation
	FAU_GEN.2. User identity association
	FAU_SEL.1. Selective audit
FDP: User Data Protection	FDP_ACC.1. Subset access control
	FDP_ACF.1. Security attribute based access control
	FDP_RIP.1. Subset residual information protection
FIA: Identification and Authentication	FIA_ATD.1. User attribute definition
	FIA_UAU.1. Timing of authentication
	FIA_UID.1. Timing of identification
	FIA_USB_(EXT).2. Enhanced user-subject binding
FMT: Security Management	FMT_MOF.1. Management of security functions behaviour
	FMT_MSA.1. Management of security attributes
	FMT_MSA.3. Static attribute initialization
	FMT_MTD.1. Management of TSF data
	FMT_REV.1(1). Revocation (user attributes)
	FMT_REV.1(2). Revocation (subject, object attributes)
	FMT_SMF.1. Specification of Management Functions
	FMT_SMR.1. Security roles

FPT: Protection of the TSF	FPT_TRC.1. Internal TSF consistency
FTA: TOE Access	FTA_MCS.1. Basic limitation on multiple concurrent sessions
	FTA_TSE.1. TOE session establishment

IDENTIFICATION

Product: Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647

Security Target: Security Target of Huawei GaussDB 100 V300R001C00B300 (version: 0.6, date: 2020-10-10).

Protection Profile: Protection Profile for Database Management Systems (Base Package), Version 2.12, 23/03/2017 (BSI-CC-PP-0088-V2).

Evaluation Level: Common Criteria v3.1 R5 - EAL2 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647 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 4.3.

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 4.4.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647, although the agents implementing attacks have the attack potential according to the basic attack potential of EAL2 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 documented in the Security Target, section 4.2.

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 categorized in the Security Target, section 5.2.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical scope of the TOE contains all interfaces and functions within the physical scope.

The following list contains all the functions and their descriptions:

- Security Audit

  Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.

- User Data Protection

  The TOE provides a discretionary access control policy to provide fine-grained access control between users and database objects. Once data is allocated to a resource, the previous information content is no longer available.

- User Identification and Authentication

  Users must identify and authenticate prior to TOE access. Attributes are maintained to support the access control policy.

- Security Management

  The TOE provides management capabilities via SQL statements. Management functions allow the administrators to configure auditing and access control options (including granting

and revoking privileges), configure users (including the maximum number of concurrent sessions) and roles, and configure primary and standby options.

- Protection of the TSF

  The database supports maximum protection mode, which ensures that data is consistently replicated to a secondary DBMS server without losing any data.

- TOE Access

  The number of concurrent user sessions may be limited by policy. Information on successful and unsuccessful login attempts is collected and user login may be restricted based on user identities, dates, and IP addresses.

PHYSICAL ARCHITECTURE

The GaussDB 100 is a software-only TOE, the physical scope of the TOE includes the TOE binary and the TOE guides. All of them are included in a DVD-ROM.

The main package that is contained in the DVD-ROM delivered to the customer by a transport shipment company is "GAUSSDB100-V300R001C00B300-EULER20SP3-64bit_release.tar.gz". And the TOE binary is a database server program named *zengine* in the package labelled as "GAUSSDB100-V300R001C00B300-DATABASE-EULER20SP3-64bit.tar.gz".

Package item	SHA-256 hash
GAUSSDB100-V300R001C00B300-EULER20SP3-64bit_release.tar.gz	6a402bb2706cb5bf7a4c5b216c117bd51735fb2a4838d82a2bd9dfe8b06fb66f
GAUSSDB100-V300R001C00B300-DATABASE-EULER20SP3-64bit.tar.gz	ce16737ae0a9b8d1acb27f5317a84ef4907ee9e8db92572f303057765cc5de8e

The table in DOCUMENTS section contains all the guides that are part of the TOE.

DOCUMENTS

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

Document name	SHA-256 hash
AGD_PRE of Huawei GaussDB 100 V300R001C00B300 V0.5.doc	5E214668D59B2E245002B5563636466C93F353DFD63BF8B5508BBC1A7F0F8B2F
AGD_OPE of Huawei GaussDB 100 V300R001C00B300 V0.5.doc	345EE25A930B79491C74CD065A9DCA264BBC09582433AEE09F27129EC3D619B1
GaussDB 100 V300R001C00B300 Feature Description 03.pdf	FD54E2F2C64745B63F56C265C74F75D9A56A8F18BD85065AB17E7666F9FFDF86

GaussDB 100 V300R001C00B300 Product Description 03.pdf	AAD41993F7DC3A4F69704655606B357A2C167C7BB9F6759C138B5C52F4E113DE
GaussDB 100 V300R001C00B300 R&D Documentation 06.pdf	43886F33B6C8D9B73E922AE2779BE8A4F720D740E4FF757C705DAAE7B040A263
GaussDB 100 V300R001C00B300 Security Hardening Guide 04.pdf	D8C7F3D5C6E3D27E4EAEA20AE70D4CE99C32D8C9110BAFE62A68EFE8C3402149
GaussDB 100 V300R001C00B300 Security Maintenance Guide 03.pdf	012A17C976E732FF19A8E3D16B3379B449D2629D54BACEC67CF263A60DC675BD
GaussDB 100 V300R001C00B300 Security Technical White Paper 03.pdf	56560FB470DA65EFD77FE1B18AB2F324957290BFE9B566246421061BBD7D3FF5
GaussDB 100 V300R001C00B300 User Guide 05.pdf	03FE43963A2BB544DA957327D9F0FB2D379108E2E78C4D911500A96983CE46CE
Security Target of Huawei GaussDB 100 V300R001C00B300 V0.6.pdf	51C62C983BC5F321EC3BC03F90579BBBEB6053BF54913CFAC0AD8106AA4655CF

PRODUCT TESTING

The developer has executed tests for all the security functions, TSFi and subsystems of the TOE. The developer in its premises, with a satisfactory result, has performed all the tests.

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.

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 basic.

The results obtained when executing the penetration tests demonstrates that the TOE [TOEV300R001C00B300] does not present exploited vulnerabilities in the operational environment defined in Security Target of Huawei GaussDB 100 V300R001C00B300 (version: 0.6, date: 2020-10-10).

Nevertheless, it is very important to strictly follow the guidance in order to avoid some potential vulnerabilities. Specifically, the section 6.6 of the guide "AGD_PRE of Huawei GaussDB 100 V300R001C00B300 V0.4".

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647 it is necessary the disposition of the following software components:

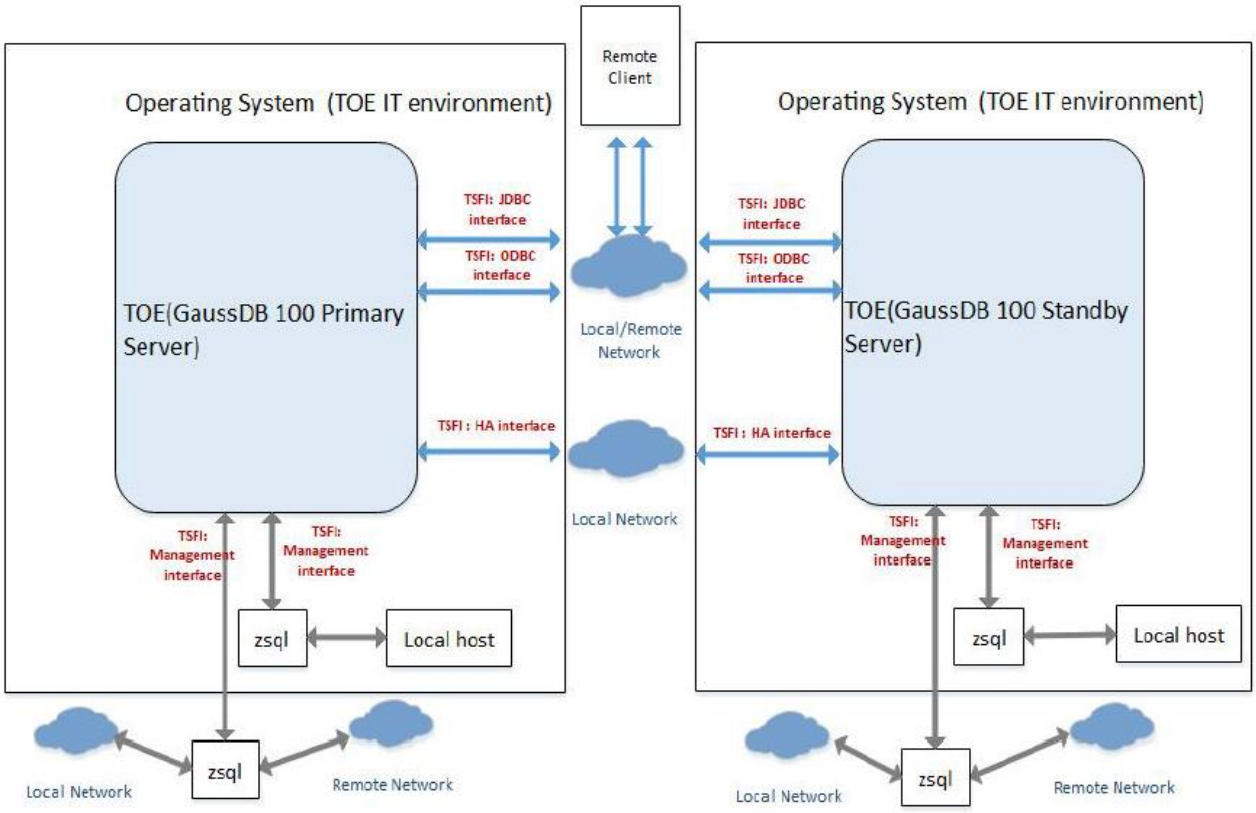
- The operating system (OS) (EulerOS Server V2.0SP3 (EulerOS), x86_64).
- JDK 8u144.
- Python v2.7.5.
- Putty v0.73.
- UnixODBC-2.3.7.

Regarding the hardware components, the requirements are:

- CPU (Specifications higher than 4 cores and 2.0 GHz are recommended)
- Memory (8 GB or larger memory is recommended.)
- Hard disk (At least 25 GB disk space is required to install the database. You are advised to reserve more than 70% of the space for data storage.)
- OS type and version
    - Evaluation OS:
        - EulerOS Server V2.0SP3 (EulerOS), x86_64
    - Supported OSs:
        - Red Hat Enterprise Linux Server release 7.4(Red Hat), x86_64
        - SUSE Linux Enterprise Server 12.4 (SUSE 12) , x86_64
        - EulerOS Server V2.0SP3 (EulerOS), x86_64
        - EulerOS Server V2.0SP5 (EulerOS), x86_64
        - EulerOS Server V2.0SP8 (EulerOS), ARM_64

Although Huawei GaussDB 100 V300R001C00B300 Release 3da6647 supports two physical deployment modes, client/database configuration and primary/standby database configuration, the

evaluated configuration has been the primary/standby database configuration, which is the one covered by this certification.



EVALUATION RESULTS

The product Huawei GaussDB 100 Version V300R001C00B300 Release 3da6647 has been evaluated against the Security Target Security Target of Huawei GaussDB 100 V300R001C00B300 (version: 0.6, date: 2020-10-10).

All the assurance components required by the evaluation level EAL2 + 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 EAL2 + ALC_FLR.2, 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 given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- 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 DEKRA Testing and Certification S.A.U., a positive resolution is proposed.

Nevertheless, it is very important to strictly follow the guidance in order to avoid some potential vulnerabilities. Specifically, the section 6.6 of the guide “AGD_PRE of Huawei GaussDB 100 V300R001C00B300 V0.4”.

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.

[BSI-CC-PP-0088-V2]Protection Profile for Database Management Systems (Base Package), Version 2.12, 23/03/2017 (BSI-CC-PP-0088-V2)

[ST06] Security Target of Huawei GaussDB 100 V300R001C00B300 (version: 0.6, date: 2020-10-10)

[AGD_PRE04] AGD_PRE of Huawei GaussDB 100 V300R001C00B300 V0.4

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Security Target Security Target of Huawei GaussDB 100 V300R001C00B300 (version: 0.6, date: 2020-10-10).

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 all assurance components selected.

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 SOGIS-MRA for all assurance components selected.