Reference: 2022-34-INF-4109- v1
Target: Limitada al expediente
Date: 18.09.2023

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

CERTIFICATION REPORT

Dossier #	**2022-34**
TOE	**Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1**
Applicant	**600413485 - Microsoft Corporation**
References	
	[EXT-7898] Certification request

Certification report of the product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1, as requested in [EXT-7898] dated 19/07/2022, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8507] received on 04/05/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1.

The TOE is the database engine of SQL Server 2022. SQL Server is a Database Management System (DBMS).

Developer/manufacturer: Microsoft Corporation.

Sponsor: Microsoft Corporation.

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

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

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4 + ALC_FLR.3.

Evaluation end date: 01/06/2023

Expiration Date[1]: 15/09/2028

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 + ALC_FR.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1, a positive resolution is proposed.

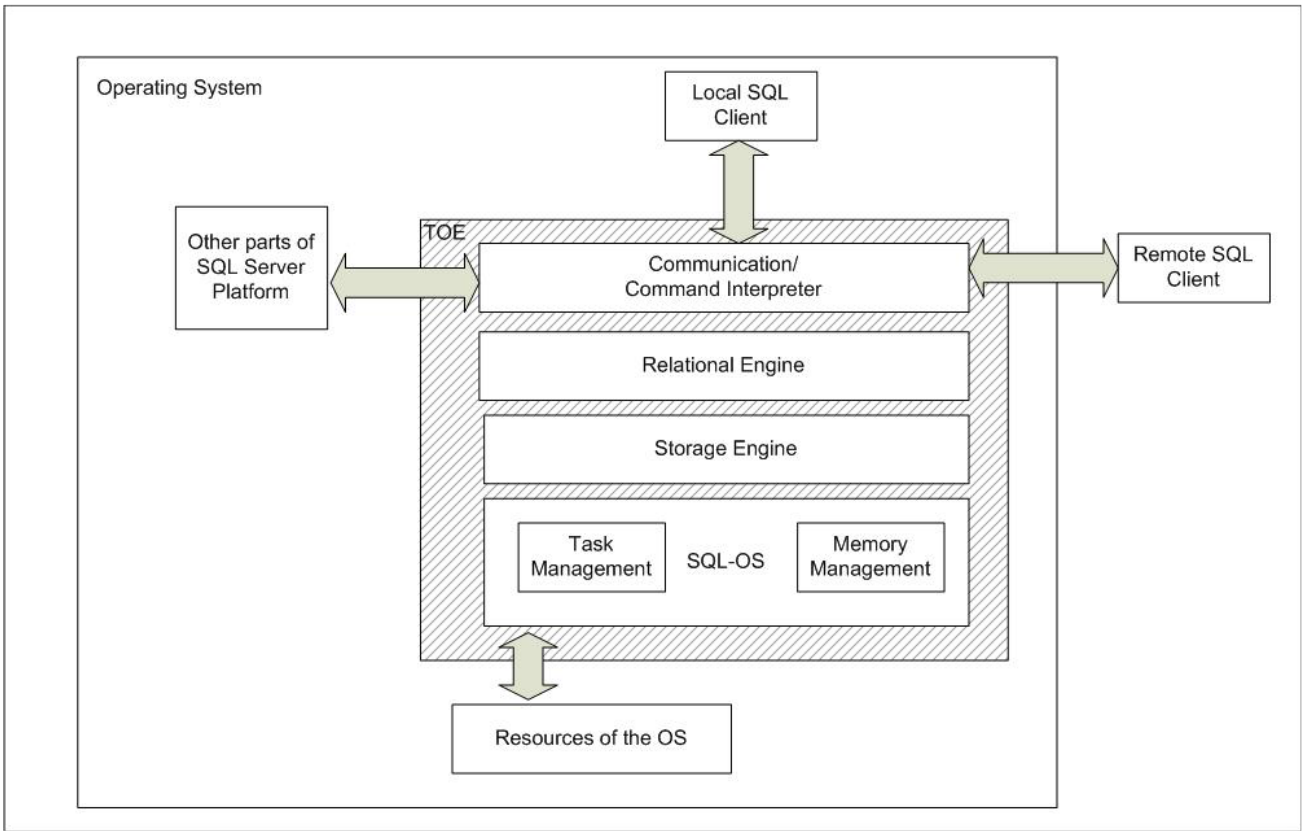
TOE SUMMARY

The TOE is the database engine of the SQL Server 2022 and its related guidance documentation. This engine is only available for x64 platforms. The comprises one instance of the SQL Server 2022 database engine but has the possibility to serve several clients simultaneously.

SQL Server 2022 is available in different editions but only the Enterprise Edition (EE) is subject to this evaluation.

The following figure shows the TOE (including its internal structure) and its immediate environment.

[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.



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, 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 v3.1 R5, including some extended components:

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SEL.1	Selective audit
Class 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
Class 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
Class 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
Class FPT: Protection of the TSF	
FPT_TRC.1	Internal TSF consistency
Class FTA: TOE Access	
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_TAH_EXT.1	TOE access information
FTA_TSE.1	TOE session establishment

IDENTIFICATION

Product: Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1

Security Target: Microsoft SQL Server 2022 Database Engine Common Criteria Evaluation (EAL4+) Security Target (v1.3, 14/04/2023).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5, EAL4 + ALC_FLR.3.

SECURITY POLICIES

The use of the product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1 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 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 3.2 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1, although the agents implementing attacks have the attack potential according to the *Enhanced Basic* 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 Security Target, section 3.3 (“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

SQL Server 2022 is able to run multiple instances of the database engine on one machine. After installation, one default instance exists. However, the administrator is able to add more instances of SQL Server 2022 to the same machine.

The TOE comprises one instance of SQL Server 2022 running on a DBMS-server. If more than one instance of SQL Server 2022 is installed on one machine these just represent multiple TOEs as there is no other interface between two instances of the TOE than the standard client interface. In this way two or more instances of the TOE may only communicate through the standard client interface.

The TOE provides the following set of security functionality through SQL-commands (via shared memory, named pipes and TCP/IP):

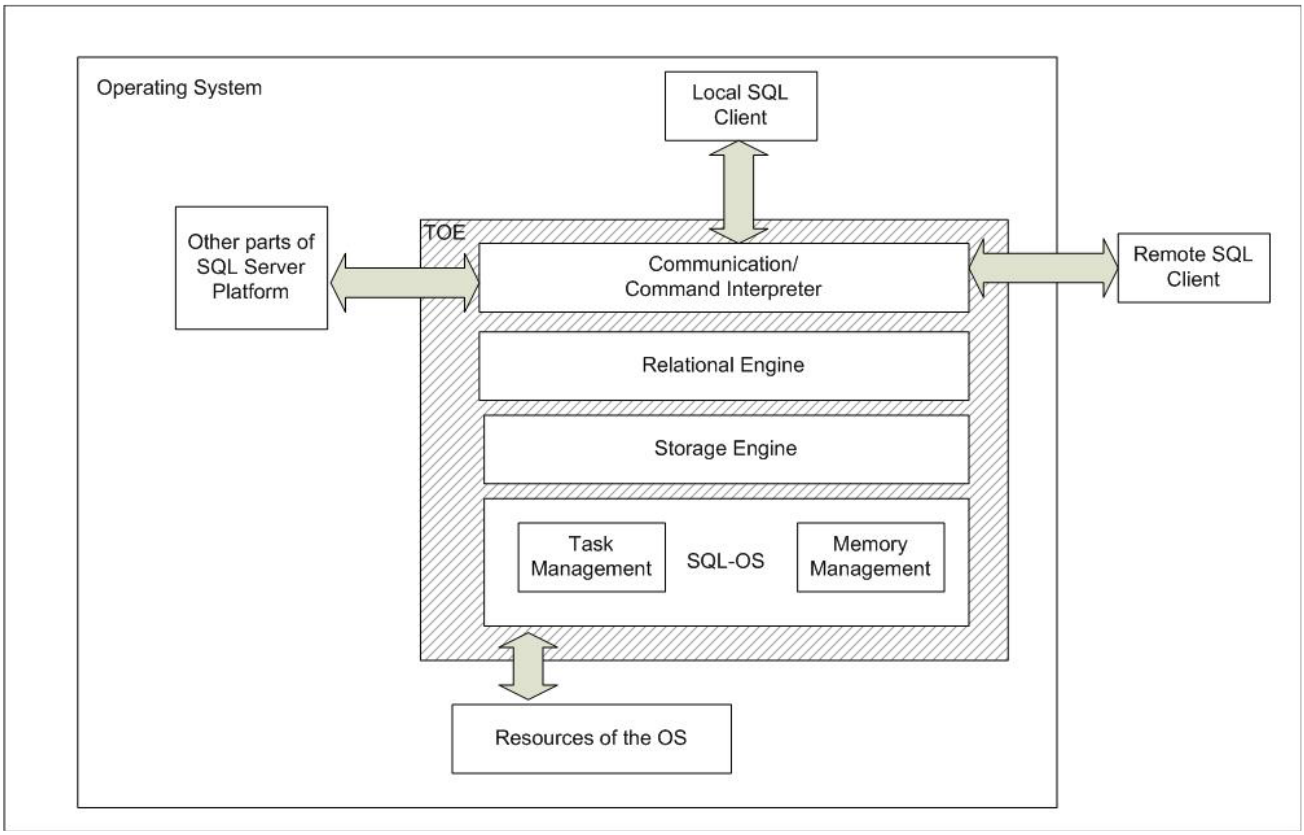
- The **Access Control** function of the TOE controls the access of users to user and metadata stored in the TOE. It further controls that only authorized administrators are able to manage the TOE.
- The **Security Audit** function of the TOE produces log files about all security relevant events.
- The **Security Management** function allows authorized administrators to manage the behaviour of the security functionality of the TOE.
- The **Identification and Authentication** function of the TOE is able to identify and authenticate users.
- The **Session Handling** mechanism which limits the possibilities of users to establish sessions with the TOE and maintains a separate execution context for every operation. Also, the Memory Management functionality belongs to the area of Session Handling and ensures that any previous information in memory is made unavailable before the memory is used either by overwriting the memory explicitly with a certain pattern or by overwriting the memory completely with new information.

PHYSICAL ARCHITECTURE

The TOE physical scope comprises both the software packages detailed below and the documents listed in the next section.

- **The TOE** (in its base version) is downloadable as a DVD image (.iso file) via the Microsoft volume licensing service center:
    - URL: https://www.microsoft.com/licensing/servicecenter/default.aspx
- **The applicable cumulative update** (CU3) is downloadable as an executable file (.exe file) via the Microsoft Update Catalog website:
    - URL: https://www.catalog.update.microsoft.com/Search.aspx?q=sql%20server%202022
    - File name: *SQLServer2022-KB5024396-x64.exe* (SHA1 value may be included as part of the filename)
    - SHA-256 value: FD9412F77876358473E08C9866F1678DDDC66739A2A9E81C8EC6514D61577405
- **Installer Triggers Script**: SQL script to install the necessary login triggers and it is provided in .sql format.
    - URL: https://www.microsoft.com/en-us/sql-server/data-security
    - File name: *SQL22_W_Install_cc_triggers_1.0_2022-12-20.sql*
    - SHA-256 value: 043AC79021C549AB198BE5DB18AC7AE160C0624AA9C870D6F606FA68BE7987C5
- **Integrity Check Validation Data**: File containing a hash verification script which can be used by customers to verify the TOE integrity and it is provided in .bat format.
    - URL: https://www.microsoft.com/en-us/sql-server/data-security
    - File name: *hash_dir_1.0_2022-12-20.bat*
    - SHA-256 value: BD9E61C4DCE7775B7999CC313124B5C94770873F49E268880E4206F508B18AEA

The figure below shows the TOE and its operational environment:



DOCUMENTS

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

- **The website** https://www.microsoft.com/en-us/sql-server/data-security (click on "View our Common Criteria certification" and a PDF document will be downloaded) contains additional information about the TOE and its evaluated configuration. Also, the guidance addendum that describes the specific aspects of the certified version can be obtained via this website. The guidance addendum extends the general guidance of SQL Server 2022. This website shall be visited before using the TOE.
- **Microsoft SQL Server 2022 Guidance Addendum**: This document contains the aspects of the guidance that are specific to the evaluated configuration of SQL Server 2022 and it is provided in .pdf format. It is the main document and should be downloaded first.
    - URL: https://www.microsoft.com/en-us/sql-server/data-security
    - File name: *SQL22_EAL4-W_AGD_ADD_1.2.pdf*
    - SHA-256 value: C62A9D1ED067D2319AF92026E5F39607ED81CAE3734A44E4B04455404D6E57A9

- **Microsoft SQL Server 2022 Technical Documentation**: This is the general guidance documentation for the complete SQL Server 2022 platform and it is provided in .zip format.
    - URL: https://www.microsoft.com/en-us/sql-server/data-security
    - File name: *Offline-Book_SQL-Server-2022_1.0_2022-12-23.zip*
    - SHA-256 value: FBB163468C5088CECD0D0808D3BAC9261FCC8CD77E8C8EB8F0F4C6AA2061EE39
- **Microsoft SQL Server 2022 Permission Poster**: This document contains all the possible permissions which apply to SQL Server 2022 and it is provided in .pdf format. Please, note that although the permission poster refers to SQL Server 2017 is also applicable for the evaluated TOE.
    - URL: https://www.microsoft.com/en-us/sql-server/data-security
    - File name: *Microsoft_SQL_Server_2017_and_Azure_SQL_Database_permissions_infographic.pdf*
    - SHA-256 value: 4C2119AD0CB54B388D900590351FEB53758139EE6574B50EAB6BEF6192EC368B

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 in the testing platform implemented in the evaluation facility.

In addition, the lab has devised a test for each of the TSFi 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 software and hardware requirements are summarized in section *PHYSICAL ARCHITECTURE* of this certification report. TOE consumers shall be provided with all the documents identified in section *DOCUMENTS*.

The TOE was evaluated using the following server configuration:

- TOE running on Windows Server 2022 Standard Edition and with Azure Arc-extension enabled.

The steps for the installation process of the TOE in its certified version can be found in the document *Microsoft SQL Server 2022 Guidance Addendum.*

EVALUATION RESULTS

The product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1 has been evaluated according to the Security Target Microsoft SQL Server 2022 Database Engine Common Criteria Evaluation (EAL4+) Security Target (v1.3, 14/04/2023).

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 + ALC_FLR.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 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 evaluation team recommends the usage of the TOE given that there are not exploitable vulnerabilities under its operational environment. They also give the following usage recommendations:

- 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 and the cumulative update in a proper manner.
- It is mandatory to strictly follow the steps indicated in the installation documentation in order to harden the TOE disabling the *xp_dirtree* stored procedure.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.
- 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.

COMMENTS & RECOMMENDATIONS FROM THE CERTIFIER

Considering the obtained evidences during the instruction of the certification request of the product Microsoft SQL Server 2022 Database Engine Enterprise Edition x64 (English) version 16.0.4025.1, a positive resolution is proposed.

The certifier recommends to potential TOE consumers to observe the *COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM*, strictly following the TOE guidance listed in section *DOCUMENTS* and to analyse the assumptions defined in the security problem definition in section 3.2 of the [ST].

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

TSFi TOE Security Functionality interface

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.

[ST] Microsoft SQL Server 2022 Database Engine Common Criteria Evaluation (EAL4+) Security Target (v1.3, 14/04/2023).

SECURITY TARGET

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

- Microsoft SQL Server 2022 Database Engine Common Criteria Evaluation (EAL4+) Security Target (v1.3, 14/04/2023).

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 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: https://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.