Reference: 2022-33-INF-4305- v1
Target: Pública
Date: 03.06.2024

Created by: CERT10
Revised by: CALIDAD
Approved by: JEFEAREA

# CERTIFICATION REPORT

| | |
|---|---|
| Dossier # | **2022-33** |
| TOE | **Microsoft SQL Server 2022 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2** |
| Applicant | **600413485 - Microsoft Corporation** |
| References | |
| | [EXT-7896] Certification request |
| | [EXT-8957] Evaluation Technical Report |

Certification report of the product Microsoft SQL Server 2022 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2, as requested in [EXT-7896] dated 19/07/2022, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8957] received on 07/03/2024.

# CONTENTS

# EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Microsoft SQL Server 2022 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2

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**: Collaborative Protection Profile for Database Management Systems, Version 1.3, March 13, 2023.

**Evaluation Level**: Common Criteria v3.1 R5, EAL2 + ALC_FLR.3.

**Evaluation end date**: 02/04/2024

**Expiration Date[1]**: 15/05/2029

All the assurance components required by the evaluation level EAL2 (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 EAL2 + ALC_FLR.3, as defined by the Common Criteria v3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Microsoft SQL Server 2022 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2, 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.

---

[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.

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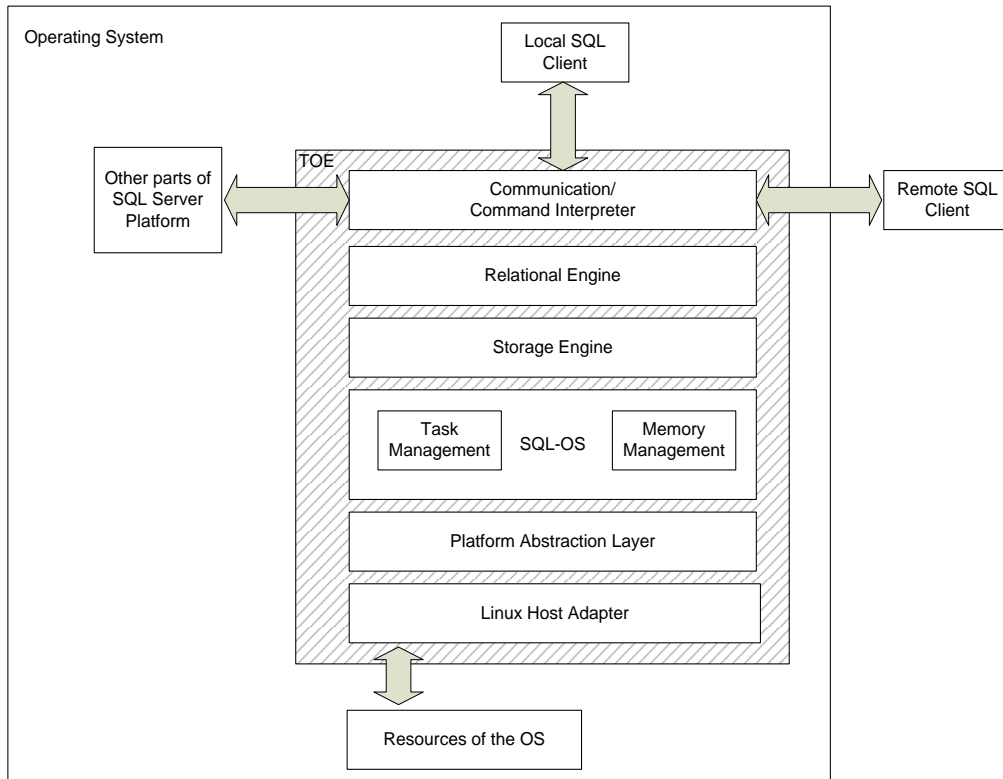


## SECURITY ASSURANCE REQUIREMENTS

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.3, according to Common Criteria v3.1 R5.

| ASSURANCE CLASS | ASSURANCE COMPONENT |
|---|---|
| ADV | ADV_ARC.1 |
|  | ADV_FSP.2 |
|  | ADV_TDS.1 |
| AGD | AGD_OPE.1 |
|  | AGD_PRE.1 |
| ALC | ALC_CMC.2 |
|  | ALC_CMS.2 |
|  | ALC_DEL.1 |
|  | ALC_FLR.3 |
| ASE | ASE_CCL.1 |
|  | ASE_ECD.1 |

| | ASE_INT.1 |
|-----|-----------|
| | ASE_OBJ.2 |
| | ASE_REQ.2 |
| | ASE_SPD.1 |
| | ASE_TSS.1 |
| ATE | ATE_COV.1 |
| | ATE_FUN.1 |
| | ATE_IND.2 |
| AVA | AVA_VAN.2 |

## SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

| 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.2 | User authentication before any action |
| FIA_UID.2 | User Identification before any action |
| FIA_USB_EXT.2 | Enhanced user subject binding |
| **Class FMT: Security Management** | |
| 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 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 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2

**Security Target:** Microsoft SQL Server 2022 on Linux Database Engine Common Criteria Evaluation (EAL2+) Security Target (version: 1.2, 2024-02-08).

**Protection Profile**: Collaborative Protection Profile for Database Management Systems, Version 1.3, March 13, 2023.

**Evaluation Level**: Common Criteria v3.1 R5, EAL2 + ALC_FLR.3.

# SECURITY POLICIES

The use of the product Microsoft SQL Server 2022 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2 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 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2, although the agents implementing attacks have the attack potential according to the *Basic* 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 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** is downloadable as a Linux installable package (.rpm or .deb) from https://packages.microsoft.com. The complete path, filename and SHA-256 value for each installable package is as follows:

- Ubuntu 20.04

| Path | https://packages.microsoft.com/ubuntu/20.04/mssql-server-2022/pool/main/m/mssql-server/mssql-server_16.0.4105.2-2_amd64.deb |
|------|------|
| Filename | mssql-server_16.0.4105.2-2_amd64.deb |
| SHA-256 | 040FF89B5B4FCEC12B827AD203EF4D2B19CFD9F08C939F61C34F0669225A50A4 |

- RHEL 8.0

| Path | https://packages.microsoft.com/rhel/8/mssql-server-2022/Packages/m/mssql-server-16.0.4105.2-2.x86_64.rpm |
|------|------|
| Filename | mssql-server-16.0.4105.2-2.x86_64.rpm |
| SHA-256 | 9B868EEC2355C563DFF30C9ADA399A374B4B911C3A835BAAC5ED399F63D931D8 |

- SLES 15

| Path | https://packages.microsoft.com/sles/15/mssql-server-2022/Packages/m/mssql-server-16.0.4105.2-2.x86_64.rpm |
|------|------|
| Filename | mssql-server-16.0.4105.2-2.x86_64.rpm |

| SHA-256 | 25AF132D01C7EB790CD1DA8288EE115500538B04FEE686EEE50EF90C10E A0536 |
|---------|---|

- **Installer Triggers Script**: SQL script to install the necessary login triggers and it is provided in .sql format.
  - o URL: https://www.microsoft.com/en-us/sql-server/data-security
  - o File name: *SQL22_L_Install_cc_triggers_1.0_2024-02-08.sql*
  - o SHA-256 value: 3149F07F76F6D1F6381ED54611841660BFA231D7AC82A952292B2568BBC926D6

The figure below shows the TOE and its operational environment:
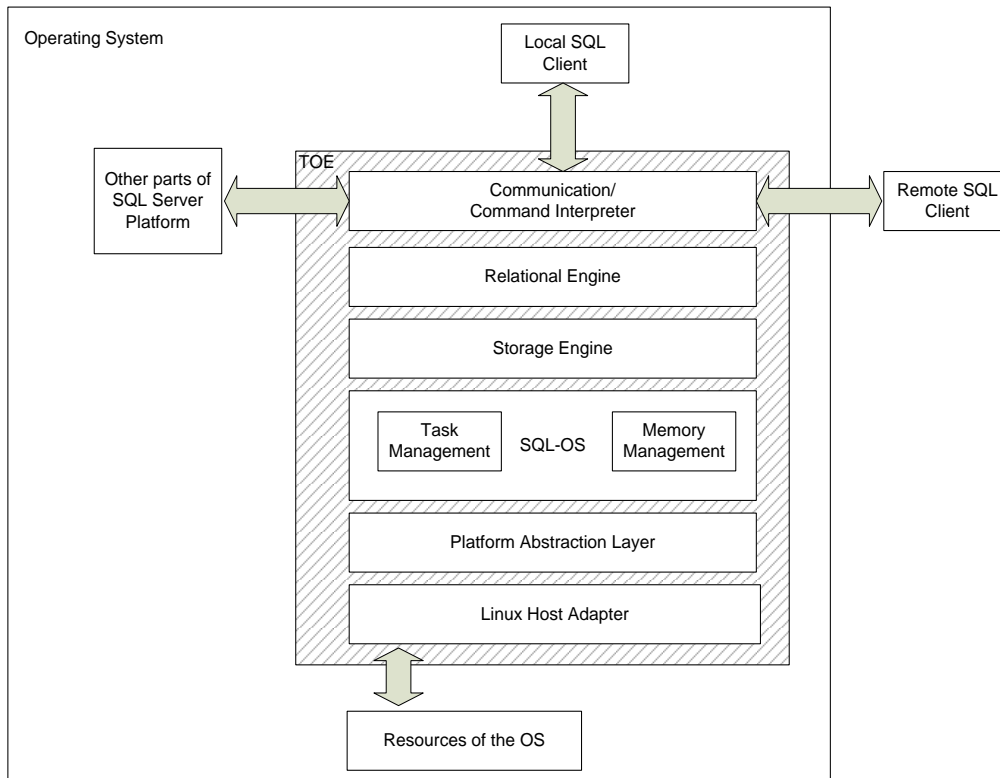


## DOCUMENTS

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. <u>This website shall be visited before using the TOE.</u>

- **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.
  - o URL: https://www.microsoft.com/en-us/sql-server/data-security
  - o File name: *SQL22_EAL2-L_AGD_ADD_1.1.pdf*
  - o SHA-256 value:
    1C97B50190B40BF64120BC2501046A6DDAACE043B949878C5C4F42F2B4FC760F

- **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.
  - o URL: https://www.microsoft.com/en-us/sql-server/data-security
  - o File name: *Offline-Book_SQL-Server-2022_1.0_2024-02-08.zip*
  - o SHA-256 value:
    48F2CFD270B05AA56945A2A0ADF6DBDB23FF667E6C52852FF42E95F178CC6909

- **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.
  - o URL: https://www.microsoft.com/en-us/sql-server/data-security
  - o File name:
    *Microsoft_SQL_Server_2017_and_Azure_SQL_Database_permissions_infographic.pdf*
  - o 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 Ubuntu Linux Server 20.04 with Azure Arc-extension enabled.

- TOE running on Ubuntu Linux Server 20.04 with Azure Arc-extension disabled.

- TOE running on Red Hat Enterprise Linux 8 with Azure Arc-extension enabled.

- TOE running on Red Hat Enterprise Linux 8 with Azure Arc-extension disabled.

- TOE running on SUSE Linux Enterprise Server v15 with Azure Arc-extension enabled.

- TOE running on SUSE Linux Enterprise Server v15 with Azure Arc-extension disabled.

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 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2 has been evaluated against the Security Target: Microsoft SQL Server 2022 on Linux Database Engine Common Criteria Evaluation (EAL2+) Security Target (version: 1.2, 2024-02-08).

All the assurance components required by the evaluation level EAL2 + 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 EAL2 + 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.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Microsoft SQL Server 2022 on Linux Database Engine Enterprise Edition x64 (English) version 16.0.4105.2, 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

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 on Linux Database Engine Common Criteria Evaluation (EAL2+) Security Target (v1.2, 08/02/2024).


# SECURITY TARGET

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

- Microsoft SQL Server 2022 on Linux Database Engine Common Criteria Evaluation (EAL2+) Security Target (version: 1.2, 2024-02-08).

# RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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: 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 selected.