Reference: 2019-45-INF-3781- v1
Target: Pública
Date: 21.04.2022

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

CERTIFICATION REPORT

Dossier #	**2019-45**
TOE	**Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1**
Applicant	**600413485 - Microsoft Corporation**
References	
	[EXT-5410] Certification request
	[EXT-7668] Evaluation technical report

Certification report of the product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1, as requested in [EXT-5410] dated 30/09/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-5410] received on 25/03/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification of the product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1.

SQL Server is a Database Management System (DBMS). SQL Server 2019 is available in different editions but only the Enterprise Edition (EE) is subject to this evaluation. The TOE is the database engine of SQL Server 2019 Enterprise Edition.

The TOE has the capability to limit TOE access to authorized users, enforce Discretionary Access Controls on objects under the control of the database management system based on user and/or role authorizations, and to provide user accountability via audit of users' actions.

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:

- DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017 (strict conformance), and
- DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017

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

Evaluation end date: 29/03/2022

Expiration Date[1]: 19/04/2027

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 + ALC_FLR.3, 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.

[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.

Considering the obtained evidences during the instruction of the certification request of the product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1, a positive resolution is proposed.

TOE SUMMARY

The TOE is the database engine of SQL Server 2019. SQL Server is a Database Management System (DBMS). The type of the TOE is a database management system (DBMS) with the capability to limit TOE access to authorized users, enforce discretionary access controls on objects under the control of the database management system based on user and/or role authorizations, and to provide user accountability via audit of users' actions.

The security functionality of the TOE comprises:

- Security Management: The TOE has the ability to restrict the access to security management functions only to authorized administrators.
- Access Control: The TOE provides the capability to restrict the access to the data and functionality to authorized users.
- Identification and Authentication: The TOE requires that each user must be successfully identified and authenticated before allowing any other actions. The TOE is also able to maintain a list of security attributes belonging to individual users.
- Security Audit: The TOE has the ability to generate and collect audit data regarding all security relevant events. Authorized administrators can also configure the audit system to exclude or include potentially auditable events to be audited based on a wide range of characteristics.
- Session Handling: The TOE provides the mechanisms to limit the possibilities of users to establish sessions with the TOE and maintain a separate execution context for every operation.

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 for Information Technology Security Evaluation Version 3.1 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:

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_TAH_(EXT).1. TOE access information
	FTA_TSE.1. TOE session establishment

IDENTIFICATION

Product: Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1

Security Target: Microsoft SQL Server 2019 Database Engine Common Criteria Evaluation (EAL4+) Security Target (version: 1.5, date: 2022-03-25).

Protection Profile:

- DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017, and
- DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017

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

SECURITY POLICIES

The use of the product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1 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 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1, 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.

The threats covered by the security properties of the TOE are those defined in the Security Target [ST15], section 3.3 (“Threats”).

For any other threat not included in the [ST15], the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

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

ARCHITECTURE

LOGICAL ARCHITECTURE

SQL Server 2019 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 2019 to the same machine.

If more than one instance of SQL Server 2019 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.

So, the TOE comprises one instance of SQL Server 2019.

The TOE provides the following set of security functionality:

- 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.

Access to the complete functionality of the TOE is possible via a set of SQL-commands.

This set of commands is available via:

- Shared Memory
- Named Pipes
- TCP/IP

PHYSICAL ARCHITECTURE

The TOE is the database engine of the SQL Server 2019 and its related guidance documentation. This engine is only available for x64 platforms. The comprises one instance of the SQL Server 2019 database engine but has the possibility to serve several clients simultaneously

Further, SQL Server 2019 is available in different editions. Only the Enterprise Edition (EE) is subject to this evaluation.

The Figure 1 shows the TOE (including its internal structure) and its immediate environment.

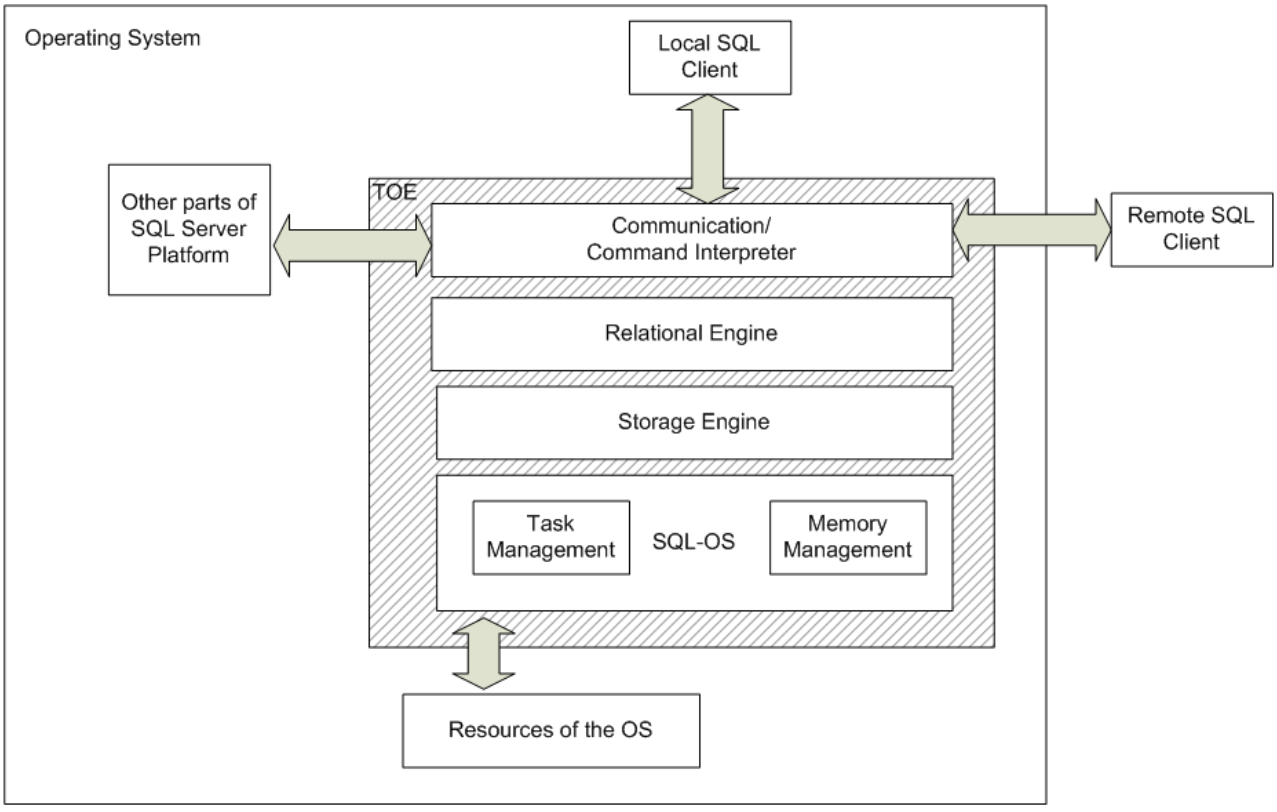

Figure 1

As seen in Figure 1 the TOE internally comprises the following units:

- The **Communication** part is the interface for programs accessing the TOE. It is the interface between the TOE and clients performing requests. All responses to user application requests return to the client through this part of the TOE.

- The **Relational Engine** is the core of the database engine and is responsible for all security relevant decisions. The relational engine establishes a user context, syntactically checks every Transact SQL (T-SQL) statement, compiles every statement, checks permissions to determine if the statement can be executed by the user associated with the request, optimizes the query request, builds and caches a query plan, and executes the statement. The Relational Engine allows compiling a subset of T-SQL statements into native code to create natively compiled Stored Procedures. The Visual C compiler used for this native compilation is not part of the TOE.
- The **Storage Engine** is a resource provider. When the relational engine attempts to execute a T-SQL statement that accesses an object for the first time, it calls upon the storage engine to retrieve the object, put it into memory and return a pointer to the execution engine. To perform these tasks, the storage engine manages the physical resources for the TOE by using the Windows OS.
- The **SQL-OS** is a resource provider for all situations where the TOE uses functionality of the operating system. SQL-OS provides an abstraction layer over common OS functions and was designed to reduce the number of context switches within the TOE. SQL-OS especially contains functionality for Task Management and for Memory Management.
- For **Task Management** the TOE provides an OS-like environment for threads, including scheduling, and synchronization - all running in user mode, all (except for I/O) without calling the Windows Operating System.
- The **Memory Management** is responsible for the TOE memory pool. The memory pool is used to supply the TOE with its memory while it is executing. Almost all data structures that use memory in the TOE are allocated in the memory pool. The memory pool also provides resources for transaction logging and data buffers.

The TOE is downloadable as a DVD image (.iso file) via the Microsoft volume licensing service center.

URL	https://www.microsoft.com/licensing/servicecenter/default.aspx
Filename	SQLServer2019-x64-ENU.iso
SHA-256	*See section 3.2.1 in [AGD_ADD]*

In addition, the Cumulative Update 13 (CU13) is downloadable via Microsoft Download Center website.

URL	https://www.microsoft.com/en-us/download/details.aspx?id=100809
Filename	SQLServer2019-KB5005679-x64.exe

SHA-256	B5EC792CABFD905B8CFDF39F2F80F4CFC987D2BC87AEF1C7F682CF452ECF02EE

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. In addition, 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 2019. This website shall be visited before using the TOE.

The following guidance documents and supportive information belonging to the TOE can be obtained through (the downloaded PDF contains the download links):

- **Microsoft SQL Server 2019 Guidance Addendum**
  - Description: This document contains the aspects of the guidance that are specific to the evaluated configuration of SQL Server 2019 ([AGD_ADD]).
  - Filename: SQL19_EAL4-W_AGD_ADD_1.3.pdf
  - SHA-256: 893CDAF7310DAE93836FC2B91156E9FABE73682ED97B7CD2695B04F3DA1018A4
- **Microsoft SQL Server 2019 Technical Documentation**
  - Description: This is the general guidance documentation for the complete SQL Server 2019 platform.
  - Filename: Offline-Book_SQL-Server-2019-CU13_1.0_2021-10-25.zip
  - SHA-256: 0B71EDCAC4969F54792DA507BBA233334A677DF1233F39F0AD7F6DD180D230E8
- **Microsoft SQL Server 2019 Permission Poster**
  - Description: This document contains all the possible permissions which apply to SQL Server 2019. NOTE: Although the permission poster refers to SQL Server 2017 is also applicable for the evaluated TOE.
  - Filename: Microsoft_SQL_Server_2017_and_Azure_SQL_Database_permissions_infographic.pdf
  - SHA-256: 4C2119AD0CB54B388D900590351FEB53758139EE6574B50EAB6BEF6192EC368B
- **Installer Triggers Script**

- Description: SQL script to install the necessary login triggers.
- Filename: SQL19_W_Install_cc_triggers_1.0_2020-05-07.sql
- SHA-256: 043AC79021C549AB198BE5DB18AC7AE160C0624AA9C870D6F606FA68BE7987C5

- **Integrity Check Validation Data Script**
  - Description: Script for verification of integrity of the TOE.
  - Filename: hash_dir_1.0_2020-05-07.bat
  - SHA-256: BD9E61C4DCE7775B7999CC313124B5C94770873F49E268880E4206F508B18AEA

PRODUCT TESTING

The developer has executed tests for all the security functions, TSFi and subsystems. 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 test case checking that the security functionality that covers was 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 addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests. Within these activities, all aspects of the security architecture, which were not covered by functional testing, have been considered.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Enhanced Basic has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer in the security guidance defined in DOCUMENTS section are applied.

The public vulnerabilities considered for the evaluation belong to the period from the TOE release in 2019 to December 10th, 2021.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1 it is necessary the disposition of the following software components:

- A host machine running Windows Server 2019 (English), Standard Edition
- Microsoft .NET Framework 4.6.2
- Windows PowerShell 3.0 or higher

The evaluator has installed and configured the TOE and its environment according to the [ST15]. [AGD_ADD] gives proper steps to carry out the installation and configuration of the TOE and its environment that is consistent with [ST15].

EVALUATION RESULTS

The product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1 has been evaluated against the Security Target Microsoft SQL Server 2019 Database Engine Common Criteria Evaluation (EAL4+) Security Target (version: 1.5, date: 2022-03-25).

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 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.

- 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 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.

COMMENTS & RECOMMENDATIONS FROM THE CERTIFIER

Considering the obtained evidences during the instruction of the certification request of the product Microsoft SQL Server 2019 Database Engine Enterprise Edition x64 (English), version 15.0.4178.1, a positive resolution is proposed.

The CCN Certification Body strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents, taking special care of the specific aspects that shall be considered when operating SQL Server 2019 in its certified version included in document [AGD_ADD] *Microsoft SQL Server 2019 Database Engine Common Criteria Evaluation – Guidance Addendum*.

The user of this TOE should pay special attention to these considerations:

- The user role *public* grants EXECUTE permissions by default but the TOE administrator must revoke such permissions on all stored procedures from *public* (see [AGD_ADD] section 8.2).
- To strictly follow the instructions from Section 3.2.5 in [AGD_ADD] in order to enable the certified version.
- This certification only includes the database engine of SQL Server 2019. The machine-learning service among other services, which are part of the SQL Server platform (see *1.4 Product Description* from [ST15]), are not included in the evaluated configuration. Therefore, those services are out of the scope of the certification.
- Per default, the connections to the database engine are not encrypted and the encryption features of SQL Server 2019 have not been considered during the evaluation. Thus the administrator has to ensure that all connections to the database engine are appropriately protected, e.g. by using and enforcing an encrypted connection or by using a physically secured connection.
- The Service Broker and Database Mirroring endpoints can be used to circumvent the Security Functionality of the TOE. Therefore, the administrator shall not install applications on the TOE that make the TSF or any data controlled by the TSF accessible through these endpoints. The administrator is not allowed to install applications on the TOE that make the TSF or any data controlled by the TSF accessible through these endpoints (see [AGD_ADD, 8.4]). This ensures that these protocols cannot be used to bypass the TSF.

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:

[AGD_ADD] Microsoft SQL Server 2019 Database Engine Common Criteria Evaluation – Guidance Addendum.

[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.

[EP] DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017.

[PP] DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017.

[ST15] Microsoft SQL Server 2019 Database Engine Common Criteria Evaluation (EAL4+) Security Target (version: 1.5, date: 2022-03-25)

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

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

- Microsoft SQL Server 2019 Database Engine Common Criteria Evaluation (EAL4+) Security Target (version: 1.5, date: 2022-03-25).

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 CCRA for all assurance components up to EAL2 and ALC_FLR.