Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1050-2020

for

Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3

from

Microsoft Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1050-2020 (*)

Database Management System

Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3

from	Microsoft Corporation
PP Conformance:	Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02, 23 March 2017, BSI-CC-PP-0088-V2-2017
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 27 January 2020

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. 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.

3.1. European Recognition of 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. 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 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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. 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 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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 7 January 2020. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Microsoft Corporation.

The product was developed by: Microsoft Corporation.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 27 January 2020 is valid until 26 January 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The software-only Target of Evaluation (TOE) is defined as: Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3. This build refers to SQL Server 2017 including Cumulative Update CU16 (item 7 of table 2) and consists solely of software and by the associated guidance documentation.

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.

A DBMS is a computerized repository that stores information and allows authorized users to retrieve and update that information. A DBMS may be a single-user system, in which only one user may access the DBMS at a given time, or a multi-user system, in which many users may access the DBMS simultaneously.

The TOE is part of the SQL Server 2017 product package. It provides a relational database engine providing mechanisms for the following security functions:

- Security Management,
- Access Control,
- Identification and Authentication,
- Security Audit,
- Session Handling.

The product package of SQL Server 2017 additionally includes a set of additional tools and services which are not part of the TOE, for details please read chapter 1.3 of the Security Target [6] and chapter 8 of this report. The TOE itself comprises the database engine of the SQL Server 2017 platform which provides the security functionality described by the ST. The additional tools and services as listed in chapter 1.3 of the Security Target [6] interact with the TOE as a standard SQL client.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02, 23 March 2017, BSI-CC-PP-0088-V2-2017 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functions	Addressed issue
Security Management (SF.SM)	This Security Function of the TOE allows

TOE Security Functions	Addressed issue
	modifying the TSF data of the TOE and therewith managing the behaviour of the TSF.
Access Control (SF.AC)	This Security Function of the TOE provides Discretionary Access Control (DAC) mechanism to control the access of users to objects based on the identity of the user requesting access, the membership of this user to roles, the requested operation and the ID of the requested object.
Identification and Authentication (SF.I&A)	This security functionality requires each user to be successfully authenticated before allowing any other actions on behalf of that user. This is done on an instance level and means that the user has to be associated with a login of the TOE.
Security Audit (SF.AU)	This Security Function creates audit logs for all security relevant actions.
Session Handling (SF.SE)	After a user attempting to establish a session has been successfully authenticated by SF.I&A this security functionality decides whether this user is actually allowed to establish a session to the TOE.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

**Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English)
Version 14.0.3223.3**

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Description
1	SW	Microsoft SQL Server 2017 Enterprise Edition, Base TOE Binaries	Enterprise Edition 14.0.3223.3 Note: The release number constitutes the certified release including CU16 (item 7 in this table). The release number of the initial version (without item 7 in this table) is 14.0.1000.169	The TOE (Database Engine of Microsoft SQL Server 2017 Enterprise Edition) is part of the SQL Server 2017 product and downloadable via the Volume Licensing Service Center under https://www.microsoft.com/licensing/servicecenter/default.aspx as installable DVD ISO-image. For SQL Server 2017 different License models do exist: Enterprise Core licenses, CAL licenses, and an evaluation version (all are binary identical)
2	DOC	SQL Server Technical Documentation [10]	Filename: Offline-Book.SQL-Server-2017-CU16.zip Filesize: 178.366.823 Bytes SHA-256: c1b3f141ea98ce25d7b222a98e3efa92b2fa059143a28992bb6fd5e10900b624	SQL Server 2017 Technical Documentation contents do not come with SQL Server 2017 but have to be downloaded separately from the Common Criteria website https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification” as a PDF document
3	DOC	Guidance Addendum [9]	Version: 1.4 Filesize: 1.544.898 Bytes Filename: MS_SQL2017_G4_AGD_ADD_1.4.pdf SHA-256: e76d6cdfa5077bc591785599edede15a3886029af40ceffba66feb33c36a6df9	Guidance addendum for Common Criteria Evaluation of SQL Server 2017 and part of the TOE. Download via: https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification”.

No	Type	Identifier	Release	Description
4	SW DATA	Script for SHA-256 hash generation for SQL Server 2017 EE	Filename: hash_dir.bat Filesize: 770 Bytes SHA-256: bd9e61c4dce7775b7999cc313124b5c94770873f49e268880e4206f508b18aea	Script which creates a list of file hashes on a specified drive so they can be used by customers to verify the TOE version. Download via the SQL Server Common Criteria web page: https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification”.
5	SW	SQL script to enable certified configuration of the TOE	Filename: G24_Install_cc_triggers.sql Filesize: 23.213 Bytes SHA-256: 094bb6dc88aa11a1bb5abc1642b2bb69289013e15c99cbb13199f60a1cab0fce	File containing a T-SQL script to install the CC logon triggers. Download via the SQL Server Common Criteria web page: https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification”.
6	DOC	Permission Hierarchy	Filename: Microsoft_SQL_Server_2017_and_Azure_SQL_Database_permissions_infographic.pdf Filesize: 1.517.072 Bytes SHA-256: 4c2119ad0cb54b388d900590351feb53758139ee6574b50eab6bef6192ec368b	Downloadable archive containing information on the permission model of the TOE. Download via the SQL Server Common Criteria web page: https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification”.
7	SW	CU16	Version: 14.0.3223.3 Filename: SQLServer2017-KB4508218-x64.exe Filesize: 554.250.352 Bytes SHA-256 value: 3f2a21cb6d68db0f184416c903815d3798a3e5883e61d1a4fc78d679f9fdf15	Downloadable file containing an installer for the SQL Server 2017 CU16. Download via https://www.microsoft.com/en-us/download/details.aspx?id=56128 See also the SQL Server Common Criteria web page for corresponding file name and hash value.

Table 2: Deliverables of the TOE

Note: Although several tools and services are delivered together with the TOE, they are excluded from the TOE and are considered part of the environment. The software-only TOE comprises only the Database Engine of the SQL Server 2017 Enterprise Edition. It is delivered as part of the SQL Server 2017 Enterprise Edition product as downloadable ISO-image via the Microsoft Volume Licensing Service Center and is identifiable as stated in item 1 of the table above. Only the x64 version is subject to this certification.

The TOE environment also includes applications that are not delivered with the TOE. The TOE uses the functionality of the underlying operating system and of other parts of the TOE environment, e.g. for audit review and audit storage, for access control mechanisms, for user authentication and identification, for providing reliable time stamps, for cryptographic mechanism for hashing of passwords, and for residual information protection of memory that is allocated to the TOE. Please read the Security Target [6] chapters 1.3.4 and 3.2.

The deliverables of the TOE are secured by cryptographic hashes.

The guidance documents [9] / [10] (items 2 and 3 from above) as parts of the TOE are delivered via download from the SQL Server Common Criteria web page.

The delivery of the TOE is secured by an integrity check procedure with hash values. The integrity verification of the TOE and of its deliverables (see Table above) is the essential part of the acceptance procedure. Prior to the TOE installation the administrator shall verify the integrity of the installation media and downloads obtained from the TOE website following the instructions on that website and in [9], chapter 3.3. In general the delivery and verification process is done via the following steps:

- Download of Microsoft SQL Server 2017 Enterprise Edition (version 14.0.1000.169) from Microsoft Volume Licensing Service Center https://www.microsoft.com/licensing/servicecenter/default.aspx.
- The SQL Server Common Criteria web page shall be visited before using the TOE and instructions shall be followed.
- Download of hash_dir.bat from https://www.microsoft.com/en-us/sql-server/data-security (link “View our Common Criteria certification”) and verification of its integrity before starting the download process via calculation of its SHA-256 hash value (using any tool capable of calculating SHA-256 hash values) and check against the reference SHA-256 hash value provided on the SQL Server Common Criteria web page or in this report.
- Download of the Guidance Addendum [9] and verification of its integrity via SHA-256 hash value calculation (using hash_dir.bat tool) and check against the reference SHA-256 hash value provided on the SQL Server Common Criteria web page or in this report. After successful verification the instructions in the Guidance Addendum [9], chapter 3.3 can be followed.
- Download of "Integrity Check Validation Data", the “Permission hierarchy”, “Books Online Guidance” and “Install_CC_triggers” via the SQL Server Common Criteria web page and verification of their integrity via SHA-256 hash value calculation (using hash_dir.bat tool) and check against the reference SHA-256 hash values provided in [9], chapter 3.3.1.
- Integrity verification of SQL Server 2017 installation ISO image (version 14.0.1000.169 without CU16) via usage of the script “hash_dir.bat”. The script checks the signature of the files and generates a list of file hashes on a specified drive so they can be used by customers to verify the TOE version. Follow the further instructions in [9], chapter 3.3.

The deliveries as identified in the table above are provided for customers/users who purchase the product and therewith the TOE. Beside the listed items there are no additional corrections that are part of the TOE and the evaluation.

The secure product homepage and the Guidance addendum [9] detail these instructions.

To determine the TOE version one has to enter the T-SQL statement "SELECT @@VERSION" and "GO". The TOE will return the name of the product platform “Microsoft SQL Server 2017” of which the TOE is the central part, the version number of the TOE, and information about the operating system. If the response to this command particularly includes "Microsoft SQL Server 2017 Enterprise Edition; 14.0.3223.3, x64" the correct TOE version, i.e. the TOE provided for evaluation, has been installed.

3. Security Policy

The security policies of the TOE are to provide authorized administrators roles to isolate administrative actions and to provide administrators with the necessary information for secure management. Furthermore the TOE provides the capability to detect and create records of security relevant events associated with users. The TOE also provides all functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. The TOE will also provide a mechanism for identification and authentication of users, and for their session handling, and will protect user data in accordance with its security policy.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The topics that are of relevance can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE consists of the following subsystems:

Protocols: This component is the communication layer of the database engine and provides the external interface for communication with a local or remote SQL client.

Execution Runtime: This component is the core of the database engine. It processes and executes user queries, invokes the security checks and performs parts of the audit functionality.

Filter Daemon Host: This component is responsible for accessing, filtering, and word breaking data from tables, as well as for word breaking and stemming the query input.

Security: This component is the core of the database engine in terms of security. It provides the functions for Access Control, Identification and Authentication and Session Handling.

Metadata: This component provides functions for the rest of the database engine to access the TSF data which is stored in system tables of the TOE.

Storage and Buffer Pool: This component is a resource provider for the other components of the TOE and provides services for storage of data, backup and restore and transaction.

Memory Management: This component provides memory allocation and management to the rest of the TOE.

SQLOS: The SQLOS component provides means to handle audit events, task scheduling services and a large range of synchronization primitives to the rest of the engine.

The IT-environment consists of the hardware platform and the underlying operating system Windows Server 2012 R2 Update (English) including KB2919355, Standard Edition or Microsoft Windows Server 2016 (English) Standard Edition). The IT-environment also consists of the other parts of the SQL Server 2017 platform, and of the clients that interact with the TOE.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

All developer tests in the context of the evaluation have been conducted on a single server installation of the database engine of Microsoft SQL Server 2017 version 14.0.3223.3 (x64) (i.e. including SP1).

The tests were run on an Intel Xeon CPU E5-2650 v4 with 2.2GHz and the operating system Windows Server 2016 Standard Edition (English) x64, as well as on on an Intel Xeon CPU E5-2650 v4 with 2.2Ghz and the operating system Windows Server 2012 R2 Standard (English). A single server installation of the database engine of SQL Server 2017 was performed according to the instructions and guidance given in [9].

The developer's testing approach was to systematically test the TOE security functionality / TSFI, i.e. the following five security functionalities as defined in [6] have been tested:

- Security Management (SF.SM),
- Access Control (SF.AC),
- Identification and Authentication (SF.I&A),
- Security Audit (SF.AU),
- Session Handling (SF.SE).

In order to do this, the developer selected a subset of the tests that were produced during the development of the TOE, which is suitable to sufficiently cover the TSF. The main testing tool is a proprietary test suite within which all tests can be executed. The test cases are divided into groups which are assigned to the security functionalities of the TOE. A test case thereby consists of several test steps which are executed sequentially and which results are compared to the expected results. Only if the results of all test steps are equal to the expected result, the test case passes.

The evaluator tests were run on Intel Xeon CPU E5-2650 v4 machines with 2.20GHz and with Windows Server 2012 R2 Standard Edition (English) x64 and Windows Server 2016

(English) Standard Edition x64. The TOE was installed according to the instructions and guidance given in [9].

The evaluator's objective was to test the functionality of the TOE systematically against the security functionality description in [6] and in the Functional Specification. In order to do this, the evaluators repeated the developer tests and devised and executed own functional tests. The evaluators performed automated tests using batch files as well as manual tests. Tests for all of the security functions were carried out. The evaluators also devised and conducted penetration tests after an independent vulnerability analysis. The evaluators created a list of potential vulnerabilities applicable to the TOE in its operational environment based on the evaluation evidence and public knowledge of vulnerabilities. Then penetration tests were devised for the relating attack scenarios. Furthermore the evaluators applied network security scans. Automatic tests using shell and Python scripts, as well as fully manual tests were performed. The penetration tests are related to the following areas: brute force attacks on identification and authentication, stored procedures parameter parsing and processing, information contained in public views, robustness of identification and authentication, vulnerability exposing programming errors, password strength, network vulnerability, bypassing of access rights, and privilege escalation.

During the TSF tests by the developer and evaluator the TOE operated as expected. The tests demonstrate that the security functions perform as expected.

During the penetration testing the TOE operated as expected. The vulnerabilities are not exploitable in the intended environment for the TOE. The TOE is resistant to vulnerabilities of Enhanced-Basic attack potential.

8. Evaluated Configuration

The Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is Microsoft SQL Server 2017 Database Engine Enterprise Edition x64 (English) Version 14.0.3223.3.

Not part of the TOE but part of the product package of SQL Server 2017 are tools, applications, and services. Although they are delivered together with the TOE, they are excluded from the TOE and are considered part of the IT-environment. The clients are also considered part of the IT-environment. Please read the Security Target, chapter 1.3 for a description of the product type, the physical and logical scope of the TOE and the boundaries of the TOE.

The document „Guidance addendum“ [9] describes the evaluated configuration and the necessary set-up to achieve the evaluated configuration.

Microsoft SQL Server 2017 is a complex software product. Therefore, it must be remembered that the TOE is the database engine only and thus the TOE environment includes many applications and services that are part of the product package but not part of the actual TOE, e.g. SQL Server Replication, Analysis Services, Reporting Services, Integration Services, Management tools, Development tools, Graphical User Interfaces, Internationalisation (Only the English version of SQL Server is evaluated), Encryption features, Clustered configuration etc. Please read the Security Target [6], chapter 1.3.1.

The product allows certain modes of operation. The modes of operation which are permitted within the certified configuration are documented in the „Guidance addendum“ [9], chapter 5.1 and have to be set as specified.

The SQL Server Common Criteria homepage is:

https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification”.

It gives instructions for a secure download and delivery of all TOE deliverables and gives necessary hash values for a verification of the TOE integrity. It also links to the downloads of all TOE deliverables.

The TOE is running on the operating system Windows Server 2012 R2 Update (English) including KB2919355, Standard Edition or Microsoft Windows Server 2016 (English) Standard Edition. The TOE itself has to be installed and configured following all instructions and guidance addendum given in [9].

For this evaluation the TOE was tested on the machines and OS as stated in chapter 7 of this report.

The TOE also uses functionality of the underlying operating system and of other parts of the TOE environment, e.g. for audit review and audit storage, for access control mechanisms, for user authentication and identification (however please note that the TOE as well as the environment provides a mechanism for identification and authentication, see chapter 7 of the ST [6]), for providing reliable time stamps, for cryptographic mechanism for hashing of passwords, and for residual information protection of memory that is allocated to the TOE. Please read the Security Target [6], chapters 1.3.4 and 3.2.

For HW- and SW-Requirements please read the Security Target [6], chapter 1.3.2.

The TOE is delivered through the web and is accessible through the secure product homepage. For more details please read chapter 2 of this report.

It has to be noted that the certification according to Common Criteria is only valid for the database engine of SQL Server 2017 Database Engine as defined in chapter 1 of this report.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02, 23 March 2017, BSI-CC-PP-0088-V2-2017 [8]

- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The administrator should verify that all software installed on the TOE server (other than the TOE itself) operates as intended.

Also, as there are no Microsoft or Third Party clients included in the evaluation, the user or administrator should verify that the client used to access the TOE operates as specified.

The user of the TOE has to be aware of the existence and purpose of the document “Guidance addendum” [9]. Therefore, the TOE’s Internet product homepage (see below) has to provide information about the existence of the document and describe how to access the document. The reference has to be unambiguous and permanent.

The developer must publish the secure product homepage

https://www.microsoft.com/en-us/sql-server/data-security and click on “View our Common Criteria certification”.

The product homepage must contain all information for a secure download and verification of the TOE items including hash values as specified in this report and all links to the TOE items as specified in this report, see table 2 in chapter 2.

The links as well as the hash values are required for verification of the components along with the descriptions for a secure download and the hash value calculation and comparison tool. They have to be present throughout the validity of this certificate.

The Guidance and the Guidance Documentation Addendum contain necessary information about the secure administration, configuration, and usage of the TOE and all security hints therein have to be considered.

The Guidance Addendum [9], chapter 3 and the secure product homepage advise the user how to download and verify the integrity of the TOE components.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CLR	Common Language Runtime
COTS	Commercial Off The Shelf
CU	Cumulative Update
DBMS	Database Management System
DC	Datacenter (Edition)
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
EE	Enterprise Edition
FCIV	File Checksum Integrity Verifier
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OS	Operating system
PP	Protection Profile
SAR	Security Assurance Requirement
SDK	Software Development Kit
SF	Security Function
SFP	Security Function Policy

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
T-SQL	Transact-SQL
XML	Extensible Markup Language

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017

Part 3: Security assurance components, Revision 5, April 2017 https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1050-2020, Microsoft SQL Server 2017 Database Engine Common Criteria Evaluation Security Target (EAL4+); Version 1.4; Date 2019-11-15; Microsoft Corporation

[7] Evaluation Technical Report (ETR), Version 2, Date: 2019-12-18; Certification ID: BSI-DSZ-CC-1050; SQL Server 2017 Database Engine Enterprise Edition x64 (English) 14.0.3223.3, (confidential document)

[8] DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, BSI-CC-PP-0088-V2, Version 2.12, March 23rd, 2017 and DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), BSI-CC-PP-0088-V2, Version 1.02, March 23rd, 2017

[9] SQL Server 2017 Database Engine - Common Criteria Evaluation (EAL4+) - Guidance Addendum; Version 1.4; Date: 2019-11-15; Microsoft Corporation

[10] SQL Server 2017 Database Engine - Common Criteria Evaluation (EAL2+) - SQL Server Technical Documentation, File name: Offline-Book.SQL-Server-2017-CU16.zip; Filesize: 178.366.823 bytes; Date: 2019-09-09; Microsoft Corporation

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report