Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1004-2017

for

Microsoft SQL Server 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0

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-1004-2017 (*)

Database Management System

Microsoft SQL Server 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0

SOGIS
Recognition Agreement

from	Microsoft Corporation
PP Conformance:	Base Protection Profile for Database Management Systems (DBMS PP) Version 2.07, 9 September 2015, BSI-CC-PP-0088-2015
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

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 4

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
for components up to
EAL 4

Bonn, 7 February 2017

For the Federal Office for Information Security

Joachim Weber
Head of Division

L.S.

Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] 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.

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

Contents

A. Certification

1. 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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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[5] [1] also published as ISO/IEC 15408.
- 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]

2. 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.

2.1. 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.

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

[3] 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

[4] 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

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

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.sogisportal.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.

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

2.2. 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 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.

This certificate is recognized according to the rules of CCRA-2014, i.e. up to and including CC part 3 EAL 2 components. The evaluation contained the components above EAL 2 that are not mutually recognised in accordance with the provisions of the CCRA-2014, for mutual recognition the EAL 2 components of these assurance families are relevant.

3. 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 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft SQL Server 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 February 2017. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] 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.

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 7 February 2017 is valid until 6 February 2022. 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,
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,

[6] Information Technology Security Evaluation Facility

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.

5. Publication

The product Microsoft SQL Server 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] 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 Target of Evaluation (TOE) is Microsoft SQL Server 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0 (including Service Pack 1) (named SQL Server 2016 hereinafter).

SQL Server 2016 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 2016 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 2016 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 2016 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 2.07, 9 September 2015, BSI-CC-PP-0088-2015 [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 modifying the TSF data of the TOE and therewith managing the behaviour of the

TOE Security Functions	Addressed issue
	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 1.3.4 and 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 3.2, 3.3 and 3.4.

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 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Description
1	SW	Microsoft SQL Server 2016, Base TOE Binaries	Enterprise Edition 13.0.1601.5 (The evaluated TOE version is 13.0.4001.0 and will be achieved after Service Pack 1 installation.)	The TOE (Database Engine of Microsoft SQL Server 2016 Enterprise Edition) is part of the SQL Server 2016 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 2016, different License models do exist: Enterprise Core licenses, CAL licenses, and an evaluation version (all are binary identical). The evaluated TOE version is 13.0.4001.0 and instantiated after Service Pack 1 installation (see next entry in this table).
2	SW	Microsoft SQL Server 2016 Service Pack 1 (SP1) (English) TOE Update	Version: 13.0.4001.0 Filename: SQLServer2016SP1-KB3182545-x64-ENU.exe Filesize: 578.604.224 bytes SHA-1: 8c6cf18878931d8efd44b952e79420002b8a4885	Executable file for the installation of SP1 for SQL Server 2016. Download from https://www.microsoft.com/en-us/download/confirmation.aspx?id=54276
3	DOC	SQL Server Books online [10]	Filename: SQL Server 2016 Technical Documentation.exe Filesize: 64.745.984 Bytes SHA-1: e04d103ea377e7ce824eed74f818743ce973abd1	SQL Server 2016 Books Online. The Documentation has to be downloaded from the Common Criteria website https://www.microsoft.com/sqlserver/en/us/common-criteria.aspx as a self-extracting archive. After unzipping the content files to a folder they can be installed to be viewed with Microsoft Help Viewer 2.2 which ships, e.g., with SQL Server Management Studio (SSMS) which is publicly available from Microsoft.

No	Type	Identifier	Release	Description
4	DOC	Guidance Addendum [9]	Microsoft SQL Server 2016 Common Criteria Certification – Guidance Addendum Version: 1.3 Date: 2016-12-21 Filesize: 1.582.669 bytes Filename: MS_SQL2016_F4_AGD_ADD_1.3.pdf SHA-1: 424f2c28c0578f046ef7756f4ad67d30fab12d87	Guidance addendum for Common Criteria Evaluation of SQL Server 2016 and part of the TOE. Download via: https://www.microsoft.com/sqlserver/en/us/common-criteria.aspx
5	SW DATA	SHA-1 hash values for SQL Server 2016 EE, containing a Verification script and Reference values	Filename: integritycheck_SQL2016.zip Filesize: 42.219 bytes SHA-1: 88f8cf8840300d6f28b2f437ebddb6334af126a5	Files containing SHA-1 hash values and script which can be used by customers to verify the TOE version. Download via the SQL Server Common Criteria web page: https://www.microsoft.com/sqlserver/en/us/common-criteria.aspx
6	DATA	SQL script to enable certified configuration of the TOE	Filename: F24_Install_cc_triggers.sql Filesize: 23.213 bytes SHA-1: 39c42c08552b036c5c489b3d679d05e704d20bf6	SQL Script to install the login triggers. Download via the SQL Server Common Criteria web page: https://www.microsoft.com/sqlserver/en/us/common-criteria.aspx
7	DOC	Permission Hierarchy	Filename: Permissions_Poster_2016_and_SQLDB.pdf Filesize: 579.066 bytes SHA-1: a781c914f8734c7f072b9ccac591b52527c6a3ee	Downloadable archive containing information on the permission model of the TOE. Download via the SQL Server Common Criteria web page: https://www.microsoft.com/sqlserver/en/us/common-criteria.aspx

No	Type	Identifier	Release	Description
8	SW	FCIV tool, TOE verification tool	Version 2.05 Filename: windows-kb841290-x86-enu.exe Filesize: 119.600 Bytes SHA-1 value: 99fb35d97a5ee0df703f0cdd02f2d787d6741f65	The FCIV tool is used to verify the integrity of the TOE together with the provided integrity check package under item 5, above. Download via: http://support.microsoft.com/default.aspx?scid=kb;en-us;841290. For further information see [9], chapter 3.3 and the secure product homepage.

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 2016 Enterprise Edition (including SP1). It is delivered as part of the SQL Server 2016 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. This engine is available in two different configurations (x86, x64). 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 3 and 4 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 2016 Enterprise Edition (version 13.0.1601.5 without SP1) 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 FCIV tool from http://support.microsoft.com/default.aspx?scid=kb;en-us;841290 and verify its integrity before starting the download process by calculation of its SHA-1 hash value (using any tool capable of calculating SHA-1 hash values) and check against the reference SHA-1 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-1 hash value calculation (using FCIV tool) and check against the reference SHA-1 hash value provided on the SQL Server Common Criteria web page or in this report. After successful verification the instructions in the Guidance Addendum can be followed.
- Download from the SQL Server Common Criteria web page the items "Integrity Check Validation Data," i.e. the SHA-1 hash values (item 5 of the table above), "Permission hierarchy," item 7 of the table above, "Books Online Guidance" [10], i.e. item 3 of the table above, and the script file "Install_CC_triggers," i.e. item 6, and verify their integrity by SHA-1 hash value calculation (using FCIV tool) by comparison with the reference SHA-1 hash values provided in [9], chapter 3.3.1.
- Integrity verification of SQL Server 2016 installation ISO image (version 13.0.1601.5 without SP1) via usage of the "Integrity Check Validation Data" (provided within the ZIP file integritycheck_SQL2016.zip in form of the XML-file “SQL2016-x64-ENU.xml” including hash values and cmd-file “integritycheck_sqlserver2016.cmd”) and following the instructions in [9], chapter 3.3.
- The SQL Server 2016 Service Pack [SP1] which is part of the evaluated version does not ship together with the product. It can be downloaded from the webpage https://www.microsoft.com/en-us/download/details.aspx?id=54276.
  Before starting the installation process for SP1, the user shall verify the integrity of the file using the FCIV tool. The verification process is described 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 2016” 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 2016 Enterprise Edition; 13.0.4001.0, 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 Datacenter Edition, Version 6.3.9600, x64 with .NET Framework 3.5 SP1. Note that .NET version 4.0 is delivered with the product installer. .NET Framework version 3.5 SP1 has to be installed separately and is therefore explicitly listed as a software requirement. PowerShell is also required but already part of the Windows Server platforms (2012 and 2016), therefore not explicitily listed as an additional software requirement. The IT-environment also consists of the other parts of the SQL Server 2016 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 2016 Database Engine Enterprise Edition x64 (English), Version 13.0.4001.0 (i.e. including SP1).

The tests were run on an Intel Xeon CPU E5504 with 2GHz, 8GB of RAM with the operating system Windows Server 2012 R2 Standard Edition (English) x64. A single server installation of the database engine of SQL Server 2016 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 a HP Compaq 8200 Elite CMT PC, Intel Core i5-2500 CPU with 3.30 GHz, 64-bit, 4GB RAM with Windows Server 2012 R2 Standard Edition (English) x64, and Intel Core2 Duo CPU E7300 with 2.66GHz, 64-bit, 4.0 GB RAM with Windows Server 2012 R2 Datacenter Edition (English) x64. Microsoft SQL Server 2016 Database Engine Enterprise Edition x64 (English), version 13.0.4001.0 (including SP1) 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 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0 (including Service Pack 1).

Not part of the TOE but part of the product package of SQL Server 2016 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 2016 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 TOE permitted modes of operation are set by a combination of certain flags, by which the TOE constitutes one instance of the Microsoft SQL Server 2016 Database Engine. These flags 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/sqlserver/en/us/common-criteria.aspx

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 Datacenter Edition, Version 6.3.9600, x64 with .NET Framework 3.5 SP1. 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 using a HP Compaq 8200 Elite CMT PC, Intel Core i5-2500 CPU with 3.30 GHz, 64-bit, 4GB RAM with Windows Server 2012 R2 Standard Edition (English) x64, and Intel Core2 Duo CPU E7300 with 2.66GHz, 64-bit, 4.0 GB RAM with Windows Server 2012 R2 Datacenter Edition (English) x64.

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 2016.

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 2.07, 9 September 2015, BSI-CC-PP-0088-2015 [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.

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/sqlserver/en/us/common-criteria.aspx

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 FCIV 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. Definitions

12.1. Acronyms

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
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
SP	Service Pack
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

12.2. 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.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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[8] 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-1004-2017, Microsoft SQL Server 2016 Database Engine Common Criteria Evaluation Security Target (EAL4+); Version 1.1; Date 2016-12-01; Microsoft Corporation

[7] Evaluation Technical Report (ETR), Version 4, Date: 2017-02-01; Certification ID: BSI-DSZ-CC-1004; SQL Server 2016 Database Engine Enterprise Edition x64 (English) 13.0.4001.0, (confidential document)

[8] DBMS Working Group Technical Community Base Protection Profile for Database Management Systems (DBMS PP), Version 2.07, 2015-09-09

[9] SQL Server 2016 Database Engine - Common Criteria Evaluation (EAL4+) - Guidance Addendum; Version 1.3; Date: 2016-12-21; Microsoft Corporation

[10] SQL Server 2016 Database Engine - Common Criteria Evaluation (EAL4+) - SQL Server Books Online; File name: SQL Server 2016 Technical Documentation.exe; Filesize: 64.745.984 bytes; Date: 2016-05-25; Microsoft Corporation

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	**Assurance Components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.