Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0698-2012

for

## Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0

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-0698-2012**

**Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0**

| | |
|---|---|
| from | Microsoft Corporation |
| PP Conformance: | U.S. Government Protection Profile for Database Management Systems, Version 1.3, 24 December 2010 |
| Functionality: | Product specific Security Target<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by ALC_FLR.2 |

Common Criteria Recognition Arrangement

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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 18 January 2012

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Joachim Weber
Head of Division

L.S.

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189 - D-53175 Bonn - 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

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:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

As of September 2011 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.Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

### 2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

## 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 Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0 has undergone the certification procedure at BSI.

The evaluation of the product Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 28 December 2011. The 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

[6] Information Technology Security Evaluation Facility

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

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 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 Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0 has been included in the BSI list of the 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

This page is intentionally left blank.

# 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 the Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0 including Service Pack 1 (named SQL Server 2008 R2 hereinafter).

SQL Server 2008 R2 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 2008 R2 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 2008 R2 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 2008 R2 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 U.S. Government Protection Profile for Database Management Systems, Version 1.3, 24 December 2010 [10].

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 Functions:

| TOE Security Functionality | 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 TSF. |
| Access Control (SF.AC) | This Security Function of the TOE provides |

| TOE Security Functionality | Addressed issue |
|---|---|
| | 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 3.2, 3.3, and 3.4.

For details about the evaluated configurations of the TOE and the configuration options relevant for a user please read chapter 8 of this report, Evaluated Configuration.

For details about necessary hardware and software requirements of the evaluated configuration please read the Security Target [6], chapter 1.3.2.

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:

**Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Description |
|---|---|---|---|---|
| 1 | SW | Microsoft SQL Server 2008 R2,<br>Base TOE Binaries | Enterprise Edition<br>10.50.2500.0 (Version including SP1) | Box and DVD-ROM of SQL Server 2008 R2 Enterprise Edition (install version); contains [8]; The TOE (Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition) is part of SQL Server 2008 R2. |
| 2 | SW | Microsoft SQL Server 2008 R2,<br>Base TOE Binaries | Datacenter Edition<br>10.50.2500.0 (Version including SP1) | Box and DVD-ROM of SQL Server 2008 R2 Datacenter Edition (install version); contains [8]; The TOE (Database Engine of Microsoft SQL Server 2008 R2 Datacenter Edition) is part of SQL Server 2008 R2. |
| 3 | DOC | SQL Server Books online [8] | Config / File / Size<br>EE & DC Edition / SQLServerBOL.msi / 184.677.376 bytes | SQL Server 2008 R2 Books Online. The installation package for Books Online is contained on the DVD that contains SQL Server itself.<br>The SQL Server Books online is part of the TOE and valid for both Enterprise Edition and Datacenter Edition. |
| 4 | DOC | Guidance Addendum [9] | Filename: MS_SQL_ AGD_ADD_1.05.pdf<br>Version: 1.05<br>SHA-1 value: ff4974f5e6c8fd303dc8de e7067e9a03eb6e465f | Guidance addendum for Common Criteria Evaluation of SQL Server 2008 R2 SP1 (valid for Enterprise Edition and Datacenter Edition).<br>The guidance addendum is part of the TOE.<br>Secure download. |
| 5 | SW | Service Pack 1 for SQL Server 2008 R2 | Config / File / Size<br>EE & DC Edition / SQLServer2008R2SP1-KB2528583-x64-ENU.exe / 324.055.392 bytes | Downloadable file containing an installer for the SQL Server 2008 R2 Service Pack 1. Updates SQL Server 2008 R2 to Version 10.50.2500.0. Serive Pack 1 is valid for both configurations: Enterprise Edition and Datacenter Edition.<br>Secure download. |

| No | Type | Identifier | Release | Description |
|---|---|---|---|---|
| 6 | SW<br>DATA<br>DOC | SHA-1 hash values for SQL Server 2008 R2,<br>Verification script, Reference values, Guidance | Config / File / Size<br>EE & DC Edition / integrity check_SQL2008R2.zip / 175.151 bytes<br>SHA-1 value: 4cd81c3458a7e0f4e8858d4527ee98e59d697a01 | Files containing SHA-1 hash values which can be used by customers to verify the TOE version (Enterprise Edition and Datacenter Edition).<br>Secure download. |
| 7 | SW | Scripts / Configuration File | Config / File / Size / SHA-1<br>EE & DC Edition / EAL4_ trace.sql / 23.335 bytes / 08e205ebafce4157cb1480aa05259de8193af84a<br>EE & DC Edition / Install_cc_ triggers.sql / 30.558 bytes / 01859d7d0c859b418896e403353a63d568b1b4d9<br>EE & DC Edition / verification_script.zip / 16.125 bytes / cebcbeb2e0a4b78ae1d14739351496af376704cc | SQL Scripts to set up the Common Criteria compliant trace process, TSF verification, and to install the necessary login triggers (valid for both configurations: Enterprise Edition and Datacenter Edition).<br>Secure download. |
| 8 | DOC | Permission Hierarchy, Guidance | Config / File / Size / SHA-1<br>EE & DC Edition / permission_hierarchy.zip / 228.836 bytes / 578bf0aa2fb56e113118b6e00ed2aec75fe95a8f | Downloadable archive containing information on the permission model of the TOE (valid for both configurations: Enterprise Edition and Datacenter Edition).<br>Secure download. |
| 9 | SW | FCIV tool, TOE verification tool | Version 2.05,<br>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 8, above.<br>Download via http://support.microsoft.com/default.aspx?scid=kb;en-us;841290<br>For further information see [8], 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.

Note: Books Online [8] is shipped together with the binaries of the TOE on a DVD. As such it inherits the version number of the TOE. The integrity of Books Online is verified using hash values as described in [9] and in the secure product homepage.

The TOE environment also includes applications that are not delivered with the TOE. The TOE uses the functionality of the underlying operating system "Windows Server 2008 R2 Enterprise Edition (English), x64," of .NET Framework 3.5 SP1, of Windows Installer 4.5, 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 a reliable time stamp, 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 download links for the TOE items 4, 6, 7, and 8 are provided on the secure product homepage:

https://www.microsoft.com/sqlserver/en/us/common-criteria.aspx

The download link for the TOE item 5 (SP1) is provided in the Guidance Addendum:

http://www.microsoft.com/downloads/details.aspx?FamilyID=B9AA2DBA-7F20-4C0C-9AFD-1EEBEE5A94EA&displaylang=pt-br&displaylang=en

The download link for the TOE items 9 is provided on the secure product homepage:

http://support.microsoft.com/default.aspx?scid=kb;en-us;841290

The secure product homepage also contains the hash value for the FCIV tool (item 9 of the list above) and for the Guidance addendum [9] (item 3 of the list above). The other hash values are provided in [9], chapter 3.3.1.

The Guidance Addendum [9] and / or the secure product homepage give instructions for the download process that are summarised hereinafter.

- Download the FCIV tool from http://support.microsoft.com/default.aspx?scid=kb;enus;841290 and verify the integrity using the provided hash value.
- Download the Guidance addendum [9] and verify its integrity via SHA-1 hash value calculation using the FCIV tool.
- Download of SHA-1 hash values (item 6 of the list above), the Configuration File (item 7 of the list above), and the Permission hierarchy (item 8 of the list above) and verify their integrity via SHA-1 hash value calculation using FCIV tool.
- Integrity verification of SQL Server 2008 R2 installation media via usage of "integrity check_SQL2008R2.zip" (containing the cmd-file “integritycheck_sqlserver2008R2.cmd”) and follow the instructions in [9], chapter 3.3.1.
- Perform an integrity verification of the SQL Server 2008 R2 Service Pack 1 installation file following the instructions in [9], chapter 3.3.3.

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 2008 R2 (SP1)” of which the TOE is the central part, the version number of the TOE, and information about the operating system. The response to this command includes the string “Microsoft SQL Server 2008 R2 (SP1) - 10.50.2500.0 (X64)“.

# 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 following topics are of relevance:

- OE.NO_EVIL: Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
- OE.NO_GENERAL_PURPOSE: There will be no general-purpose computing capabilities (e.g. compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.
- OE.PHYSICAL: Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

Details can be found in the Security Target [6], chapter 4.2.

# 5 Architectural Information

The TOE, as illustrated in Fig. 1 of chapter 1.3.2 of the Security Target [6] can be described by following components:

- The Communication / Command Interpreter is the interface for programs accessing the TOE. It is the interface between the TOE and clients performing requests. All responses to user application requests return to the client through the Communication part and Command Interpreter.
- The Relational Engine is the core of the database engine and is responsible for all security relevant decisions.
- The Storage Engine is a resource provider. It manages the physical resources for the TOE by using the Windows OS.
- The SQL-OS is a resource provider for all situations where the TOE uses functionality of the operating system.
- Task Management provides an OS-like environment for threads but without calling the Windows Operating System.
- The Memory Manager is responsible for the TOE memory pool.

The IT-environment consists of the underlying operating system and hardware platform "Windows Server 2008 R2 Enterprise Edition (English), x64," .NET Framework 3.5 SP 1, Windows Installer 4.5, as well as of the other parts of the SQL Server 2008 R2 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 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0 (including Service Pack 1) and in two configurations (Enterprise Edition and Datacenter Edition).

The tests were run on a Dell Optiplex 755 (Intel Core 2 Quad CPU x64 @2.4GHz , 8GB of RAM) with the operating system Windows Server 2008 R2 Enterprise Edition (English), Version 6.1.7600, x64. SQL Server 2008 R2 with the database engine as the TOE was installed 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’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 on a HP Proliant DL385, 2.6 GHz AMD Opteron 252 Processor (2 CPUs), 64-bit with the operating system Windows Server 2008 R2 Enterprise Edition (English), Version 6.1.7600, x64. 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

evaluator 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 evaluator applied network security scans and tool based static code analysis. Automatic tests using shell and Python scripts, as well as fully manual tests were performed.

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 the “Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64, Version 10.50.2500.0”.

Not part of the TOE but part of the product package of SQL Server 2008 R2 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 2008 R2 is a complex Software product. Therefore, it must be remembered that the TOE is the database engine 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, Internationalization (Only the English version of SQL Server is evaluated), VIA Protocol, Encryption features, Clustered Servers, Full Text Search, Business Intelligence Development Studio, Client tools connectivity, Client tools backwards compatibility, Client tools SDK, SQL client connectivity SDK, Microsoft Sync framework. Please read the Security Target [6] chapter 1.3.1.

The product 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 that are additional to the boxed DVD.

The TOE is running on the operating system "Windows Server 2008 R2 Enterprise Edition (English), x64". 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 the Server machine HP Proliant DL385, 2.6GHz AMD Opteron 252 Processor (2 CPUs), 64-bit as hardware platform.

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, for providing a reliable time stamp, 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 main part of the TOE is delivered within the SQL Server 2008 R2 product package in form of a boxed DVD (COTS product) through the sales channels. Some TOE deliverables according to table 2 of this report are delivered via the web and are accessible through its 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 2008 R2.

# 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 for those components up to EAL4 and all interpretations and guidelines of the Scheme [4].

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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: U.S. Government Protection Profile for Database Management Systems, Version 1.3, December 24, 2010 [10]
- For the Functionality: Product specific Security Target<br>Common Criteria Part 2 extended
- For the Assurance: Common Criteria Part 3 conformant<br>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 cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

# 10 Obligations and Notes for the Usage of the TOE

The operational 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 policies 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 TOE 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 for 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

**NSA** National Security Agency

**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

**VIA** Virtual Interface Adapter

**XML** Extensible Markup Language

## 12.2 Glossary

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

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

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

**Informal** - Expressed in natural language.

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

**Protection Profile** - An implementation-independent statement of security needs for a TOE type.

**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** - A set of software, firmware and/or hardware possibly accompanied by guidance.

**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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0698-2012, Microsoft SQL Server 2008 R2 Database Engine Common Criteria Evaluation, Version 1.04; Date 2011-09-26; Microsoft Corporation

[7] Evaluation Technical Report (ETR), Version: 3, Date: 2011-12-20, Certification ID: BSI-DSZ-CC-0698, Database Engine of Microsoft SQL Server 2008 R2 Enterprise Edition and Datacenter Edition (English) x64 10.50.2500.0 (confidential document)

[8] Microsoft SQL Server 2008 R2 Database Engine Common Criteria Evaluation – SQL Server Books Online; Version 10.50.2500.0; Date: 2010-04-03; Microsoft Corporation

[9] Microsoft SQL Server 2008 R2 Database Engine Common Criteria Evaluation – Guidance Addendum; Version 1.05; Date: 2011-12-08; Microsoft Corporation

[10] U.S. Government Protection Profile for Database Management Systems, Version 1.3, 24 December 2010

[8] specifically

- AIS 32, Version 7, 08.06.2011, CC-Interpretationen im deutschen Zertifizierungsschema

# C Excerpts from the Criteria

CC Part1:

**Conformance Claim**

“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<br>APE_OBJ.2 Security objectives |
| | APE_ECD.1 Extended components definition |
| | APE_REQ.1 Stated security requirements<br>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<br>ASE_OBJ.2 Security objectives |
| | ASE_ECD.1 Extended components definition |
| | ASE_REQ.1 Stated security requirements<br>ASE_REQ.2 Derived security requirements |
| | ASE_TSS.1 TOE summary specification<br>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<br>ADV_FSP.2 Security-enforcing functional specification<br>ADV_FSP.3 Functional specification with complete summary<br>ADV_FSP.4 Complete functional specification<br>ADV_FSP.5 Complete semi-formal functional specification with additional error information<br>ADV_FSP.6 Complete semi-formal functional specification with additional formal specification |
| | ADV_IMP.1 Implementation representation of the TSF<br>ADV_IMP.2 Implementation of the TSF |
| | ADV_INT.1 Well-structured subset of TSF internals<br>ADV_INT.2 Well-structured internals<br>ADV_INT.3 Minimally complex internals |
| | ADV_SPM.1 Formal TOE security policy model |
| | ADV_TDS.1 Basic design<br>ADV_TDS.2 Architectural design<br>ADV_TDS.3 Basic modular design<br>ADV_TDS.4 Semiformal modular design<br>ADV_TDS.5 Complete semiformal modular design<br>ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation |

| Assurance Class | Assurance Components |
|---|---|
| AGD:<br>Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life cycle support | ALC_CMC.1 Labelling of the TOE<br>ALC_CMC.2 Use of a CM system<br>ALC_CMC.3 Authorisation controls<br>ALC_CMC.4 Production support, acceptance procedures and automation<br>ALC_CMC.5 Advanced support |
| | ALC_CMS.1 TOE CM coverage<br>ALC_CMS.2 Parts of the TOE CM coverage<br>ALC_CMS.3 Implementation representation CM coverage<br>ALC_CMS.4 Problem tracking CM coverage<br>ALC_CMS.5 Development tools CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures<br>ALC_DVS.2 Sufficiency of security measures |
| | ALC_FLR.1 Basic flaw remediation<br>ALC_FLR.2 Flaw reporting procedures<br>ALC_FLR.3 Systematic flaw remediation |
| | ALC_LCD.1 Developer defined life-cycle model<br>ALC_LCD.2 Measurable life-cycle model |
| | ALC_TAT.1 Well-defined development tools<br>ALC_TAT.2 Compliance with implementation standards<br>ALC_TAT.3 Compliance with implementation standards - all parts |
| ATE: Tests | ATE_COV.1 Evidence of coverage<br>ATE_COV.2 Analysis of coverage<br>ATE_COV.3 Rigorous analysis of coverage |
| | ATE_DPT.1 Testing: basic design<br>ATE_DPT.2 Testing: security enforcing modules<br>ATE_DPT.3 Testing: modular design<br>ATE_DPT.4 Testing: implementation representation |
| | ATE_FUN.1 Functional testing<br>ATE_FUN.2 Ordered functional testing |
| | ATE_IND.1 Independent testing – conformance<br>ATE_IND.2 Independent testing – sample<br>ATE_IND.3 Independent testing – complete |
| AVA: Vulnerability assessment | AVA_VAN.1 Vulnerability survey<br>AVA_VAN.2 Vulnerability analysis<br>AVA_VAN.3 Focused vulnerability analysis<br>AVA_VAN.4 Methodical vulnerability analysis<br>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.

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| 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”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 8.3)

“Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested** (chapter 8.4)

“Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked** (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed** (chapter 8.6)

“Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested** (chapter 8.7)

“Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested** (chapter 8.8)

“Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested** (chapter 8.9)

“Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

**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.”

This page is intentionally left blank

# D Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.