Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0366-2008

for

Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00

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-0366-2008

Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English)
Version 9.00.3068.00

from	Microsoft Corporation
PP Conformance:	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, version 1.1, June 7, 2006
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant 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 accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 24. October 2008
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all Evaluation Assurance Levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this agreement.

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

2.2 International Recognition of CC - Certificates

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 February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: 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.

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 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00 has undergone the certification procedure at BSI.

The evaluation of the product Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 16 October 2008. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the 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.

---

[6] Information Technology Security Evaluation Facility

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, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, 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 may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://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) and subject of the Security Target (ST) [6] is the database management system (DBMS) product “Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00”. It includes Service Pack 2 and GDR 4.

It 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.

The TOE is part of the product package of the SQL Server 2005. 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 additionally includes a set of additional tools which are not part of the TOE, for details please read chapter 2.2 of the Security Target [6].

The TOE itself comprises the database engine of the SQL Server 2005 platform which provides the security functionality described by the ST. The additional tools as listed in chapter 2.2 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 in Basic Robustness Environments,” version 1.1, June 7, 2006 [9].

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 5. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.2.

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

TOE Security Function	Addressed issue
Security Management (SF.SM)	This Security Function provides the necessary functions to change the behavior of the TSF.
Access Control (SF.AC)	This Security Function realizes the Discretionary Access Control Policy for all objects under the control of the TOE.
Identification and Authentication	This Security Function realizes the identification

TOE Security Function	Addressed issue
(SF.I&A)	and authentication function of the TOE which is used for the cases where the identity of the user has not been verified by the environment.
Security Audit (SF.AU)	This Security Function realizes the audit functionality for the TOE.
Session Handling (SF.SE)	This Security Function realizes the Session Handling.

Table 1: TOE Security Functions

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

The claimed TOE's Strength of Functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 6.1 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

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 Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

The TOE "Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00" is a portion of the product package of the SQL Server 2005 consisting of the database engine of the SQL Server 2005 platform and including the security functions Security Management, Access Control, Identification and Authentication, Security Audit, and Session Handling.

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 requirements of the evaluated configuration please read the Security Target [12], chapter 2. 2 and the Certification report of the underlying operating system [13].

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 2005 SP2,
Enterprise Edition (English) Version 9.00.3068.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Base TOE Binaries: Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English)	Version 9.00.3068.00 (after application of Service Pack 2 and GDR 4)	CD (Boxed COTS Software)
2	SW	TOE update: Microsoft SQL Server 2005 Enterprise Edition SP2 (English)	File properties name: SQLServer2005SP2-KB921896-x86-ENU.exe size: 296,157,040 bytes	Download
3	SW	TOE update: GDR 4 for SQL Server 2005 Enterprise Edition	File properties name: SQLServer2005-KB948109-x86-ENU.exe size: 27,508,752 bytes	Download
4	DOC	Guidance: SQL Server Books Online [10]	File properties name: SqlServer2K5_BOL.msi size: 141,532,672 bytes February 2007	Download
5	SW	Guidance: Guidance addendum for Common Criteria Evaluation of SQL Server 2005 SP2 [11]	File properties name: MS_SQL_AGD_IGS_1.5.pdf size: 2,034,026 bytes SHA-1 hash: b03ddbe475bd1971a16cd17ad50c96647ce6097c	Download
6	SW	Configuration File: SQL Scripts to set up the Common Criteria compliant trace process and to install the necessary login triggers	File properties name: EAL4_trace.sql size: 22,964 bytes name: Install_cc_triggers.sql size: 30,552 bytes	Download
7	SW	TOE verification tool: File Checksum Integrity Verifier (FCIV) utility	File properties name: windowskb841290-x86-enu.exe size: 119,600 bytes SHA-1hash: 99fb35d97a5ee0df703f0cdd02f2d787d6741f65	Download
8	SW	Checksums to be verified by FCIV: SHA-1 hashes	File properties name: SQL2005_SP2_EAL4_Hashes.zip size: 22,450 bytes SHA-1 hash: 9703db854eb7c295cd5654cf93b909851e918816	Download

No	Type	Identifier	Release	Form of Delivery
9	SW	Basic test to verify the correct operation of the Security Functions: Verification Scripts	File properties name: verification_script.zip size: 15,130 bytes	Download
10	DOC	Permission Hierarchy	File properties name: permission_hierarchy.zip size: 312,553 bytes	Download

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 TOE environment also includes applications that are not delivered with the TOE. The TOE uses the functionality of the underlying operating system "Windows Server 2003, Enterprise Edition, 32-bit version, SP 1", e.g. for log file storage, for audit record readability, for cryptographic operations, for user data protection, for access control functions, for user authentication and identification, and for providing a reliable time stamp. The functionality of the underlying operating system is specified in the SFRs for the IT-Environment in chapter 5.2 and Table 23 of chapter 8.7 of the Security Target [6].

For HW-Requirements please read the Security Target [6], chapter 2.2.

The delivery of the TOE is secured by cryptographic hashes.

The download links for all TOE items that are listed in the table above are provided on the secure product homepage:

https://www.microsoft.com/sql/commoncriteria/2005/sp2/default.mspx

The page also contains the hash values for the item 5 (MS_SQL_AGD_IGS_1.5.pdf), item 7 (FCIV), an item 8 (SQL2005_SP2_EAL4_Hashes.zip) of the table above. All other hash values are provided in item 8 (SQL2005_SP2_EAL4_Hashes.zip) of the table above.

The secure product homepage gives instructions for the download process that are summarised hereinafter.

- Download the FCIV tool from the link provided in the product homepage and verify its SHA-1 value using any tool capable of calculating SHA-1 values.
- Download the "Integrity Check Validation Data" (item 8 of the table above) and "CC Guidance Addendum" (item 7 of the table above) and verify the integrity by using the FCIV tool. The hash values of those two items are provided on the product homepage.
- The administrator is then advised to follow the CC Guidance Addendum ([11], item 5 of the table above) for further verification of the TOE deliverables and for the Installation and Configuration of the TOE.

The secure product homepage details these instructions.

3 Security Policy

The security policies of the TOE are to:

- define requirements for monitoring user activities and to monitor security relevant events and act as a deterrent to security violations,
- define the requirements for protecting user and TSF data from unauthorized access and unauthorized modification or deletion,
- define the requirements for identifying and authenticating users as authorized users of the TOE,
- define the requirements for managing the security of the TOE,
- define the requirements for protecting the TOE security functions from actions of untrusted subjects beyond its security domain,
- define the control and monitoring of access to the TOE.

The TOE allows 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. This can be done either on an instance level or on a database level.

The TOE 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. The TOE uses a Mixed Mode Authentication which means that there are two types of logins, i.e. Windows accounts and SQL Server logins. The administrator specifies the type of login for every login he is creating.

The TOE also features the generation of audit logs for security relevant actions as well as the permission or denial of establishing sessions, based on specific rules and on the number of allowed sessions.

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 relevant:

- 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.OS_PP_VALIDATED: The underlying OS has been validated against an NSA sponsored OS PP of at least Basic Robustness. The evaluation and certification of the underlying OS has to be done on at least EAL 4 augmented by ALC_FLR.2.
- 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.
- OE.COMM: Any communication path from and to the TOE will be appropriately secured to avoid eavesdropping and manipulation.

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

5 Architectural Information

The TOE, as illustrated in Fig. 1 of chapter 2.2 of the Security Target [6], can be described by following components:

- The Communication Part / 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, as well as of the other parts of the SQL Server 2005 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. The documentation contains the required information for secure delivery and 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 and evaluator tests in the context of the evaluation have been conducted on a single server installation of the database engine of SQL Server 2005 using the final version of the TOE. The machine used for testing was a Dell Optiplex GX270 with an Intel Pentium 4 2.6GHz CPU and 2GB RAM.

The Operating System "Windows Server 2003, Enterprise Edition, 32-bit version, SP 1" has been installed in compliance to the Windows Server 2003 Security Configuration Guide [14] and the Windows Server 2003 Evaluated Configuration Administrator's Guide [15]. This includes usage of the Security Configuration Template "CC_Baseline_W2K3.inf" from the Windows Server 2003, Security Configuration Guide [14]. The TOE itself has been installed and configured following all instructions and guidance given in [11].

A separate test client has been set up, containing the proprietary test scripts, several SQL clients, and a third-party penetration testing tool.

The main testing tool was a proprietary test suite within which all tests have been executed.

The Developer test cases are divided into groups which are assigned to the Security Functions of the TOE. Each test case consists of several test steps which are executed sequentially. All five security functions which the TOE provides have been tested.

The developer's testing results demonstrate that the TSF perform as specified. The developer's testing results demonstrate that the TOE performs as expected.

The evaluators testing was performed on a similar hardware and configuration. Of the SQL package, only the following components of SQL server were installed :

- SQL Server Database Services (Core TOE component),
- Client Components (includes Management Studio, Client tools, and Books Online), and
- Full Text Search (required for two of the developer tests).

The evaluator's objective was to test the functionality of the TOE systematically against the TSF description in the security target [6] and the functional specification. Additionally, the repetition of developer tests verified the developer's test results. All security functions of the TOE were tested.

The evaluators tested all TSF defined in the security target [6] and the functional specification. The evaluators testing included positive and negative tests.

During the evaluator's TSF tests, the TOE operated as specified. The tests demonstrate that the security functions perform as specified.

The evaluators devised and conducted penetration tests related to the developer's vulnerabilities analysis and the evaluator's Independent vulnerability analysis

The penetration tests examined all security functions. During the evaluator's penetration testing based on the developer vulnerability analysis, the TOE operated as specified. The vulnerabilities discussed in the developer vulnerability analysis are not exploitable in the intended environment for the TOE. The TOE is resistant to attackers with low attack potential.

8 Evaluated Configuration

The Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is the database management system (DBMS) product "Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00" with Service Pack 2 and GDR 4.

Not part of the TOE but part of the product package of SQL Server are tools, applications, and services such as Replication Services, Notification Services, Integration Services, Analysis Services, Reporting Services, Management Tools, Development Tools.

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 IT-environment. Please read the security target, chapters 2.1, 2.2, and 2.4 for a description of the product type, the physical and logical scope of the TOE and the boundaries of the TOE.

The document „Microsoft SQL Server TM 2005 Database Engine Common Criteria Evaluation – Guidance Addendum / Installation / Startup" [11] describes the evaluated configuration and the necessary setup to achieve the evaluated configuration. It also describes that some functions were not part of the evaluation, such as the VIA protocol, Management Studio, Graphical User Interface (e.g. SQL Configuration Manager and SQLXML Client Features), common language runtime (CLR), encryption features, support

of Windows User Interface Design and Development, Support of Windows Internationalization (the English version is evaluated), and clustered servers.

The product homepage is

https://www.microsoft.com/sql/commoncriteria/2005/sp2/default.mspx.

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 CD.

The TOE is running on the operating system "Windows Server 2003, Enterprise Edition, 32-bit version, SP 1" (build 3790, English, SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch (KB907865)).

"Windows Server 2003, Enterprise Edition, 32-bit version, SP 1" has been set up in its certified version as described in the Windows Server 2003 Security Configuration Guide, Version 1.0, September 22, 2005 [14] and the Windows Server 2003 Evaluated Configuration Administrator's Guide [15] and was configured using the Security Template "CC_Baseline_W2K3.inf" from Windows Server 2003, Security Configuration Guide [14].

The TOE itself has been installed and configured following all instructions and guidance addendum given in [11].

For this evaluation the TOE was tested using a Server machine Dell Optiplex GX270 with Intel Pentium 4 processor, 2,6GHz and 2.0 GB RAM as hardware platform.

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 2003, Enterprise Edition, 32-bit version, SP 1", e.g. for log file storage, for audit record readability, for cryptographic operations, for user data protection, for access control functions, for user authentication and identification, and for providing a reliable time stamp. The functionality of the underlying operating system is specified in the SFRs for the IT-Environment in chapter 5.2 and Table 23 of chapter 8.7 of the Security Target [6].

For more details about necessary hardware requirements of the evaluated configuration please read the Security Target [12], chapter 2. 2 and the Certification Report of the underlying operating system [13].

The Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00 is delivered in form of a boxed CD (COTS product) through the sales channels. Service Pack 2, GDR 4 as well as all other TOE deliverables according to table 2 of this report are delivered via the web only 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 2005 Enterprise Edition and with Service Pack 2 and GDR 4 only.

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 (AIS) [4] as relevant for the TOE.

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

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

The evaluation has confirmed:

- PP Conformance: U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, version 1.1, June 7, 2006 [9]
- 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 following TOE Security Functions fulfil the claimed Medium Strength of Function:
  - Identification and Authentication (SF.I&A)

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 of this report contain necessary information about the usage of the TOE and all security hints therein have to be considered. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents. Please read also chapter 8 of this report.

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 Guidance Documentation Addendum Document “Microsoft SQL Server 2005 Database Engine Common Criteria Evaluation – Guidance Addendum / Installation / Startup” [11]. 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/sql/commoncriteria/2005/sp2/default.mspx.

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 usage of the TOE and all security hints therein have to be considered.

The Guidance Addendum [11], chapter 7 lists the requirements on securely managing the TOE.

The Guidance Addendum [11], chapter 5.1 lists the modes of operation for the TOE that shall not be used within the scope of the certified version.

The Guidance Addendum [11], chapter 5 lists two modes that require special care of the administrator.

The Guidance Addendum [11], chapter 3 (with additional information in chapters 8.1 – 8.3) 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

CD Compact Disk

CC-MRA Common Criteria - Mutual Recognition Arrangement

CLR Common Language Runtime

COTS Commercial Off The Shelf

DBMS Database Management System

EAL Evaluation Assurance Level

FCIV File Checksum Integrity Verifier

GDR General Distribution Release

IT Information Technology

NSA National Security Agency

OS	Operating system
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SoF	Strength of Function
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 assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, Version 2.3, August 2005

[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, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0366: Microsoft SQL Server 2005 Database Engine Common Criteria Evaluation, Version 1.27, Date 2008-07-23, Author Microsoft Corporation

[7] Evaluation Technical Report, BSI-DSZ-CC-0366, Version 3, Date 2008-10-15 Product:Database Engine of Microsoft SQL Server 2005, Enterprise Edition (English) Version 9.00.3068.00, ITSEF: TÜVIT (confidential document)

[8] Configuration Management Microsoft SQL Server 2005 Database, Engine Common Criteria Evaluation, Version 1.3, 2008-07-25

and

List of file-names of all Source Code files of Microsoft SQL Server 2005, Enterprise Edition (English), Version 9.00.3068.00, File name: TOE_sources.xls, Size: 1184256 bytes, 2008-07-23

and

List of Binaries for Database Engine of Microsoft SQL Server 2005, Enterprise Edition (English), Version 9.00.3068.00, Size: 360573 bytes, 2008-07-23

(confidential documents)

[9] U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, version 1.1, June 7, 2006.

[10] Books Online - Microsoft SQL Server 2005 File properties – name: SqlServer2K5_BOL.msi, signing date/time: Tuesday, 13 February 2007 23:52:39, size: 141,532,672 bytes, Version: February 2007, Microsoft Corporation

[11] Microsoft SQL Server TM 2005 Database Engine Common Criteria Evaluation – Guidance Addendum / Installation / Startup, Version 1.5, Date 2008-09-26, Microsoft Corporation

[12] Microsoft Windows 2003/XP Security Target, Version 1.0. 28.09.2005, Microsoft Corporation

---

[8] specifically

- AIS1, AIS11, AIS14, AIS19, AIS23, and
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

[13] Common Criteria Evaluation and Validation Scheme Validation Report – Microsoft Windows 2003 Server and XP Workstation, National Information Assurance Partnership, Report Number: CCEVS-VR-05-0131, Version: 1.1, Date: November 6, 2005

[14] Windows Server 2003 Security Configuration Guide, Microsoft Corporation, Dated: September 22, 2005, Version: 1.0

[15] Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 1.0, 2005-09-21, Microsoft Corporation

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.