Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0416-2007

for

Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00

from

Microsoft Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0416-2007

Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00

from

Microsoft Corporation

Common Criteria Arrangement

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* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL1**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 21. March 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT
Security
Certified

SOGIS - MRA

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.

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)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), 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] 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 7 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 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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been 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 levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 (CC-MRA). 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

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 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 has undergone the certification procedure at BSI.

The evaluation of the product Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 was conducted by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor and distributor is:

Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052-6399, USA

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 21. March 2007.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for recertification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-18.

The product Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product.

[7] Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052-6399, USA

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

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 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00

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.

The product package of SQL Server additionally includes a set of additional tools which are not part of the TOE, these are Replication Services, Notification Services, Integration Services, Analysis Services, Reporting Services, Management Tools, Development Tools.

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 above interact with the TOE as a standard SQL client.

The IT product Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 was evaluated by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed on 15. March 2007. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and vendor and distributor is

Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052-6399, USA

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL1 without augmentations.

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_SEL.1	Selective audit
Class FDP: User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_REV.1(1)	Revocation (user attributes)
FMT_REV.1(2)	Revocation (subject, object attributes)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles

Table 1: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	**Addressed issue**
FAU_GEN_EXP.2	User and/or group identity association

Security Functional Requirement	Addressed issue
FAU_STG_EXP.4	Administrable Prevention of audit data loss

Table 2: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Class FAU: Security Audit	
FAU_STG.1/ENV	Protected audit trail storage
FAU_SAR.1/ENV	Audit Review
Class FCS: Cryptographic Support	
FCS_COP.1/ENV	Cryptographic Operation
Class FDP: User Data Protection	
FDP_ACC.1/ENV	Subset access control
FDP_ACF.1/ENV	Security attribute based access control
Class FIA: Identification and Authentication	
FIA_UAU.1/ENV	Timing of authentication
FIA_UID.1/ENV	Timing of identification
Class FMT: Security Management	
FMT_MSA.3/ENV	Static attribute initialisation
Class FPT: Protection of the TSF	
FPT_STM.1/ENV	Reliable time stamps

Table 3: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.2.

These Security Functional Requirements are implemented by the TOE Security Functions:

Identifier	TOE Security Function	Description
SF.SM	Security Management	This Security Function provides the necessary functions to change the behavior of the TSF.
SF.AC	Access Control	This Security Function realizes the Discretionary Access Control Policy for all objects under the control of the TOE.
SF.I&A	Identification and Authentication	This Security Function realizes the identification and authentication

Identifier	TOE Security Function	Description
		function of the TOE.
SF.AU	Security Audit	This Security Function realizes the audit functionality for the TOE.

Table 4: Security Functions

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

1.3 Strength of Function

There is no strength of functions claim for the TOE.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The TOE maintains two types of data which represent the assets: User Data and TSF Data.

The following list of considered threats for the TOE is defined in the Security Target [6], chapter 3.3:

Threats	Description
T. ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	A user or process may claim to be another entity in order to gain unauthorized access to data or TOE resources.
T.TSF_COMPROMISE	A user or process may try to access (i.e. view, modify or delete) configuration data of the TOE. This could allow the user or process to gain knowledge about the configuration of the TOE or could bring the TOE into an insecure configuration in which the security mechanisms for the protection of the assets are not longer working correctly.
T.UNAUTHORIZED_ ACCESS	A user may try to gain unauthorized access to user data for which they are not authorized according to the TOE security policy. Within the scope of this threat the user just tries to access assets, he doesn’t have permission on, without trying to masquerade another user or circumventing the security mechanism in any other way.

Table 5: Threats

There are two Security policies to be fulfilled by the TOE, please refer to the Security Target [6], chapter 3.4:

Assumption	Description
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.

Assumption	Description
P.ROLES	The TOE shall provide an authorized administrators role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

Table 6: Organisational Security Policies

1.5 Special configuration requirements

The TOE Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 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, and Security Audit.

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.

The document „Microsoft SQL Server 2005 SP1 Database Engine Common Criteria Evaluation,Guidance Addendum / Installation / Startup“ [10] 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), common language runtime (CLR) hosting, encryption functions, support of Windows User Interface Design and Development, Support of Windows Internationalization (the English version is evaluated), and clustered servers.

The TOE is running on a Microsoft Windows Server 2003 Enterprise Edition 32-bit operating system (build 3790, English, SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch (KB907865)) and was configured using the Security Template “CC_Baseline_W2K3.inf” from Windows Server 2003, Security Configuration Guide, Version 1.0, September 22, 2005.

For this evaluation the TOE was tested using a generic Server machine with Dual Processors of 2.80 and 2.81 GHz, 2.0 GB RAM, two HDDs, Keyboard, Monitor, Mouse, network card, DVD-RW drive as the hardware platform.

For more details about necessary hardware requirements of the evaluated configuration please read the Security Target [6], chapter 2. 2 and the Certification report of the underlying operating system [8].

1.6 Assumptions about the operating environment

The following assumptions concerning the operating environment are made in the Security Target, please refer to the Security Target [6], chapter 3.2:

Assumption	Description
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There are 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.
A.OS_PP_VALIDATED	The underlying OS has been validated against an NSA sponsored OS PP of at least Basic Robustness and the Operating System provides functionality for • Identification and authentication of users, • Access Control for Files, • Time stamps, • Audit Storage and Audit Review, • Hashing of passwords
A.PHYSICAL	It is assumed that appropriate physical security is provided for the server, on which the TOE is installed, considering the value of the stored, processed, and transmitted information.
A.COMM	It is assumed that any communication path from and to the TOE is appropriately secured to avoid eavesdropping and manipulation.

Table 7: Assumptions

1.7 Disclaimers

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 Enterprise Edition (English)
SP1 Version/Build 9.00.2047.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery

No	Type	Identifier	Release	Form of Delivery
1	SW (Base TOE Binaries)	Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English)	Version/Build 9.00.2047.00 (Note: TOE Version is only valid after application of Service Pack)	CD (boxed, COTS software)
2	SW (TOE update)	SQL Server 2005 Service Pack 1	File properties - name: SQLServer2005SP1-KB913090-x86-ENU.exe, size: 264.954.656 Bytes	Downloadable available from: http://www.microsoft.com/sql/commoncriteria/
3	DOC	SQL Server Books Online	July 2006, File properties - name: SqlServer2K5_BOL_Jul2006.msi, size: 129.097.728 Bytes	Downloadable available from: http://www.microsoft.com/sql/commoncriteria/
4	DOC	SQL Server Guidance Addendum / Installation / Startup	Version 1.21 / Date 2007-03-14	Downloadable available from: http://www.microsoft.com/sql/commoncriteria/
5	Configuration File	Startup script (Optional), name: EAL1_trace.sql	14/12/2006, File properties - name: EAL1_trace.sql, size: 21.435 Bytes	Downloadable available from: http://www.microsoft.com/sql/commoncriteria/

Table 8: 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 2003 Server, 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, for security management, and for providing a reliable time stamp. The functionality of the underlying operating system is specified in the security requirements for the IT environment, see chapter 1.2 of this report, SFRs for the IT-Environment, and chapter 5.2 of the Security Target [6].

3 Security Policy

The security policy of the TOE is to modify the TSF data to securely manage the TOE and its security functions by authorized administrators by applying T-SQL statements.

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.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions, the following usage condition exist. Please refer to the Security Target [6], chapter 3.2 for more detail:

- Assuming the trustworthiness and appropriate training of Administrators as well as their adherence to all administrator guidance (A.NO_EVIL).

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6], chapter 3.2):

- Assuming the provision of appropriate physical security for the server, on which the TOE is installed, considering the value of the stored, processed, and transmitted data (A.PHYSICAL)
- Assuming the non-availability of general-purpose computing capabilities (e.g. compilers or user applications) on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS (A.NO_GENERAL_PURPOSE).
- Assuming that the underlying OS has been validated against an NSA sponsored OS PP of at least Basic Robustness and that the Operating System provides functionality for Identification and authentication of users, Access Control for Files, Time stamps, Audit Storage and Audit Review, Hashing of passwords (A.OS_PP_VALIDATED).
- Assuming the protection of the communication paths to and from the TOE to avoid eavesdropping and manipulation (A.COMM).

Furthermore, the Security Target [6], chapter 3.4 defines two Organisational Security Policies:

- P.ACCOUNTABILITY states that the authorized users of the TOE shall be held accountable for their actions within the TOE.

- P.ROLES states that the TOE shall provide an authorized administrators' role for secure administration of the TOE. This role shall be separate and distinct from other authorized users

4.3 Clarification of scope

Additional threats that are not addressed by the TOE and its evaluated security functions were not addressed by this product evaluation.

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 resp. 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 following guidance documents and supportive information belong to the TOE and are provided with the product by the developer to the customer:

[9] SQL Server 2005 Books Online (July 2006), File properties - name: SqlServer2K5_BOL_Jul2006.msi, size: 129.097.728 Bytes

[10] Microsoft SQL Server 2005 SP1 Common Criteria Evaluation – Guidance Addendum / Installation / Startup, Version 1.21 / Date 2007-03-14

7 IT Product Testing

Basis of all test configurations is an installed TOE as identified in the Security Target [6]. For the testing, the TOE has been installed on a generic Server machine with Dual Processors of 2.80 and 2.81 GHz, 2.0 GB RAM, two HDDs, Keyboard, Monitor, Mouse, network card, DVD-RW drive as the hardware platform, the underlying operation system Microsoft Windows Server 2003 Enterprise Edition 32-bit operating system (build 3790, English, SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch (KB907865)).

For the ITSEF's independent testing, the TOE was installed on a machine that met the minimum requirements for both the TOE and Windows Server 2003 Enterprise Edition. 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, which is not included within the scope of evaluation)

The evaluator tests have been performed at the ITSEF facility in Essen, Germany.

All tests were performed using the tool "sqlcmd", with the exception of Audit Log Verification. The ITSEF used the provided "Profiler" tool to view and verify the audit logs.

The evaluators performed six tests using batch files. Each batch included several sub-testcases. The tests covered each TSF defined in the ST [6] and in the Functional Specification with at least one test.

During the tests, the TOE operated as specified.

8 Evaluated Configuration

The Target of Evaluation (TOE) is called Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 and is a part of the product package of the SQL Server 2005. Not part of the TOE but part of the product package of SQL Server 2005 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.

The document „Microsoft SQL Server TM 2005 SP1 Database Engine Common Criteria Evaluation,Guidance Addendum / Installation / Startup" [10] describes the evaluated configuration and the necessary setup to achieve the evaluated configuration. It also describes that several functions are not part of the evaluation, such as the VIA protocol, Management Studio, Graphical User Interface (e.g. SQL Configuration Manager), common language runtime (CLR) hosting, encryption functions, support of Windows User Interface Design and

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

The TOE is running and was tested on a Microsoft Windows Server 2003 Enterprise Edition 32-bit operating system (build 3790, English, SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch (KB907865)) and was configured using the Security Template "CC_Baseline_W2K3.inf" from Windows Server 2003, Security Configuration Guide, Version 1.0, September 22, 2005.

For this evaluation the TOE was tested using a generic Server machine with Dual Processors of 2.80 and 2.81 GHz, 2.0 GB RAM, two HDDs, Keyboard, Monitor, Mouse, network card, DVD-RW drive as the 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 2003 Server, 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, for security management, and for providing a reliable time stamp.

The Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 is delivered in form of a boxed CD through the sales channels. Service Pack 1 as well as the Guidance called "SQL Server 2005 Books Online (July 2006)" [9] and the additional Guidance Document "Microsoft SQL Server 2005 SP1 Common Criteria Evaluation – Guidance Addendum / Installation / Startup" [10] are delivered via the web only.

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 1 only.

9 Results of the Evaluation

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 identical with EAL1.

The verdicts for the CC, Part 3 assurance components (according to EAL1 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Version Numbers	ACM_CAP.1	PASS
Delivery and operation	CC Class ADO	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Tests	CC Class ATE	PASS
Independent testing – conformance	ATE_IND.1	PASS

Table 9: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended,
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL1.

The results of the evaluation are only applicable to the Database Engine of Microsoft SQL Server 2005 Enterprise Edition (English) SP1 Version/Build 9.00.2047.00 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [6] and the chapters 2, 4 and 8 of this report).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for recertification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The Guidance documentation (see chapter 6 of this report) contains necessary information about the secure usage of the TOE. 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 user of the TOE has to be aware of the existence and purpose of the Guidance Documentation Addendum Document “Microsoft SQL Server 2005 SP1 Common Criteria Evaluation – Guidance Addendum / Installation / Startup” [10]. Therefore, the TOE’s Internet product homepage 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 guidance and the Guidance Documentation Addendum contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

API	Application Programming Interface
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
DVD	Digital Versatile Disc

EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
IT	Information Technology
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
RAM	Random Access Memory
RW	Read-Write
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
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

13.2 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.

14 Bibliography

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, 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.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0416-2007, Microsoft SQL Server 2005 SP1 Database Engine Common Criteria Evaluation, Version: 1.4, 2007-01-23)

[7] Evaluation Technical Report, Version 3, Datum 2007-03-14, TÜV Informationstechnik GmbH (confidential document)

[8] Certification Report/ Validation Report, Microsoft Windows 2003 Server and XP Workstation, Report Number: CCEVS-VR-05-0131, Dated: November 6, 2005, Version: 1.1, National Institute of Standards and Technology

[9] SQL Server 2005 Books Online (July 2006), File properties - name: SqlServer2K5_BOL_Jul2006.msi, size: 129.097.728 Bytes)

[10] Microsoft SQL Server 2005 SP1 Common Criteria Evaluation – Guidance Addendum / Installation / Startup, Version 1.21, 2007-03-14

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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.