Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2015-10-19 (ITC-5563)
Certification No.	C0537
Sponsor	Microsoft Corporation
TOE Name	SQL Server 2016 Database Engine Enterprise Edition x64 (English)
TOE Version	13.0.4001.0 (including Service Pack 1)
PP Conformance	Base Protection Profile for Database Management Systems (DBMS PP), Version 2.07
Assurance Package	EAL2 augmented with ALC_FLR.2
Developer	Microsoft Corporation
Evaluation Facility	TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

This is to report that the evaluation result for the above TOE is certified as follows.

2017-02-15

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center, Technology Headquarters

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation
  Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation
  Version 3.1 Release 4

Evaluation Result: Pass

"SQL Server 2016 Database Engine Enterprise Edition x64 (English)" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1 Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "SQL Server 2016 Database Engine Enterprise Edition x64 (English)" (hereinafter referred to as the "TOE") developed by Microsoft Corporation, and the evaluation of the TOE was finished on 2016-12 by TÜV Informationstechnik GmbH, Evaluation Body for IT-Security (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Microsoft Corporation, and provide security information to procurement entities and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is provided along with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "procurement entities and general consumers who purchase this TOE that is commercially available" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL2 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

This TOE is the core area of the software components that build Microsoft's database management system (SQL Server 2016). SQL Server 2016 consists of a database engine (this TOE) with various support tools (user database management UI tools, various data analysis tools, client development aid tools, and so on) added.

This TOE provides the security functionalities required for Base Protection Profile for Database Management Systems (DBMS PP), Version 2.07 [14] (hereinafter referred to as the "conformance PP"), which is a Protection Profile for database management systems.

Regarding these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated in the scope of the assurance package. The TOE assumes threats and assumptions as described in the following sections.

1.1.2.1 Threats and Security Objectives

The TOE counters each threat with the following security functionalities.

There are various threats of disclosure and falsification through unauthorized access to protected assets, including databases that the TOE handles and setting information related to security functionality.

In order to counteract such threats, this TOE provides access control by authenticating each user to allow users to perform only their permitted operations. In addition, by generating and managing audit data related to security events, the TOE detects unauthorized operations.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

This TOE shall be installed with required software (such as OS) to operate the TOE to a dedicated server machine, and used in an environment that allows communication with other connected client machines via a network.

The server machine to which this TOE is installed shall be placed to a location physically protected from unauthorized access, and it shall be operated in a network environment where communication data between the server and the clients is protected from falsification and eavesdropping.

1.1.3 Disclaimers

The protection of the communication data between a server and a client in the TOE operational environment is outside the assurance of this evaluation, and it is operator’s responsibility to take measures.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2016-12, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document" [1], "Requirements for IT Security Certification" [2], and "Requirements for Approval of IT Security Evaluation Facility" [3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2 Identification

The TOE is identified as follows:

TOE Name:	SQL Server 2016 Database Engine Enterprise Edition x64 (English)
TOE Version:	13.0.4001.0 (including Service Pack 1)
Developer:	Microsoft Corporation

Users can verify that a product is the evaluated and certified TOE by the following means.

Users can identify the installed product as this evaluated TOE by following the procedure found in the product document to send an SQL command to obtain the TOE version of the running TOE and comparing it to the applicable description of that in the TOE configuration list.

3 Security Policy

This chapter describes security function policies employed by this TOE to counteract threats and organizational security policies.

The TOE provides security functionality to defend against unauthorized access to its internally managed database.

In order to comply with organizational security policies, the TOE has a functionality to generate audit data related to security events and properly manage the generated audit data.

It also prevents the security functionality from being disabled or abused by allowing only system administrators to configure the various security settings described above.

The assets protected by this TOE's security functionality are:

(1) Protected assets (user data)

- User information stored and managed in a database
- Query information, such as stored procedures, created by users and managed within the TOE

(2) Protected assets (major TSF data)

- Database definition information containing various information, including roles and user account mapping information
- User account information and other information related to role definition
- Various setting information related to security functionality
- Security audit data

3.1 Security Function Policies

The TOE possesses the security functionalities to counter the threats listed in Section 3.1.1., and to satisfy the organizational security policies listed in Section 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functionalities to counter them. These threats are the same as the ones written in the conformance PP.

Table 3-1: Assumed Threats

Identifier	Threat
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or process acting on behalf of a user may masquerade as another entity in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.
T.RESIDUAL_DATA	A user or process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A malicious user or process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.
T.UNAUTHORIZED_	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

3.1.1.2 Security Function Policies against Threats

All the threats shown in Table 3-1 are associated with the compromise (viewing, falsification) of user data and TSF data by unauthorized TOE users or by users without authorized rights. The TOE counters these threats by the following security function policies.

1) ID authentication functionality

It is a functionality which verifies that a user attempting to use the TOE is an authorized user, and which allows only authorized users to access the TOE. There are two mechanisms to achieve this functionality: Windows authentication and SQL Server authentication. The system administrator chooses either method for each account when creating user accounts. Details of those mechanisms are explained below.

(Windows authentication)

User account information (account security identifier, or SID) authenticated by the OS using the ID authentication functionality in the Windows OS (the host of the TOE) is obtained and mapped to the user account of the TOE.

(SQL Server authentication)

The TOE itself verifies the authenticity of a user by comparing the login name and password against user account information managed by the TOE.

Authenticated users are allowed to use the TOE based on the user role assigned to each of their accounts.

2) Security management functionality

This TOE enforces access control based on the user rights to operations related to user accounts (creation, deletion, changing rights, and so on), operations related to database access rights, and other operations including changing security settings. This TOE prevents unauthorized access by limiting these operations to users with system administrator rights only.

3) Access control functionality

This TOE manages the access control list that defines permission or denial for each database operation. By using this access control list and user account information identified by the above ID authentication functionality, the TOE defends against unauthorized access to the database by enforcing access control with the timing required for the operation from users. Details of the access control functionality are explained below.

This functionality manages the following right list for each database stored in the TOE.

- List of explicit permission or denial for certain accounts regarding each database operation (creation, modification, reference, deletion, and so on)
- List of explicit permission or denial for certain roles regarding each database operation (each role and account information belonging to each role are managed per database and related objects)

User information and these right lists are referenced every time when a database operation request (SQL) is sent to the TOE from a user via a client, and access control is enforced based on the following rules:

1. If an explicit denial on a specific operation from the user account is defined, the operation requested from that user is denied.
2. If an explicit denial on a specific operation from any role to which a user account belongs is defined, the operation requested from that user is denied.
3. If an explicit permission on a specific operation from the user account is defined, the operation requested from that user is permitted.
4. If an explicit permission on a specific operation from any role to which a user account belongs is defined, the operation requested from that user is permitted.
5. If none of the above rules apply, the operation is denied.

However, the system administrators and other users who created the databases (database owners) are permitted for all operations to the databases. For this functionality, the default roles provided in advance by the TOE (for example, db_datareader role with permission to reference all table information of the databases and db_datawriter role with permission to add, delete, and modify all table information of the databases) or other roles newly defined by the system administrators and database owners are used.

4) User session handling functionality

By using the user account information identified by the above ID authentication functionality, this TOE restricts accesses to the TOE against the security policies configured by the system administrators in advance. In the security policies, specific user accounts that restrict accesses to the TOE, date/time, day of the week, and the maximum number of concurrent sessions, are configured. When a user accesses to the TOE, the TOE determines whether to permit the subsequent user operations or not, based on these security policies.

5) Residual information overwrite functionality

In regard to the memory area where a user reuses by accessing to the TOE, it ensures that any previous residual information is made unavailable by overwriting with certain patters in advance.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE are shown in Table 3-2. These organizational security policies are the same as the ones written in the conformance PP.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functionalities to meet the organizational security policies shown in Table 3-2.

1) Means for organizational security policy "P.ACCOUNTABILITY"

This security policy requires accountability for the TOE users' operations. In order to comply with this policy, the TOE achieves accountability of the users' actions by providing the security audit functionality described as follows, generating the audit log containing all events related to the security functionality, and managing the audit log files.

- Security audit functionality

When a security event subject to audit occurs, the TOE generates an audit log including items, such as event type, user ID, date and time of the event, the result of the event, and stores this audit log as an audit log file. It also provides an interface to a system administrator to read the generated audit log files. Generated audit log files are protected by the access control functionality provided by the OS.

In addition, date/time information is obtained from the OS system clock in order to record the event date/time in the audit log.

2) Means for organizational security policy “P.ROLES”, “P.USER”

These security policies require that restrictive roles should be defined independently from those of general users in order to securely manage the TOE, and that user rights should be properly managed.

This TOE complies with these security policies by a mechanism that defines the system administrator role with administrator right related to the security functionality and that manages this role separately from those of general users, and by the security management functionality as well as the user session handling functionality described in Section 3.1.1.2.

4 Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1: Assumptions in Use of the TOE

Identifier	Assumptions
Physical aspects	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.□
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
Procedural aspects	
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.PEER_FUNC_& _MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.

Identifier	Assumptions
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.2 Environmental Assumptions

This TOE shall be installed with an OS to a server machine placed at a physically secure location, and used by the connected clients via a network.

Communication with the clients shall use the command communication tools provided by the TOE developer, development aid tools contained in the product along with the TOE, and independently developed client applications.

Hardware that comprises the server machine, related software such as the OS, and the reliability of both are beyond the scope of this evaluation (and are assumed sufficiently reliable).

Table 4-2 shows the hardware specification required for the target server machine to which the TOE is installed, and Table 4-3 illustrates required software other than the TOE.

Table 4-2: Hardware Requirements

CPU	AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support at 1.4 GHz or faster
RAM	1GB
Hard Disk	Approx. 6GB of free space
Other	DVD drive, display at S-VGA or higher resolution, pointing device, keyboard

Table 4-3: Software Requirements

OS	Windows Server 2012 R2 (English), Standard Edition or Datacenter Edition
Other software	.NET Framework 3.5 SP1

4.3 Clarification of Scope

As shown in Section 4.2, this TOE is a software product installed to a server machine.

5 Architectural Information

This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

This TOE works as one application on the operating system (OS). Figure 5-1 illustrates the internal structure of the TOE. The shaded area represents the TOE; it excludes the local SQL client, remote SQL client, other parts of SQL Server Platform, and resources of the OS.

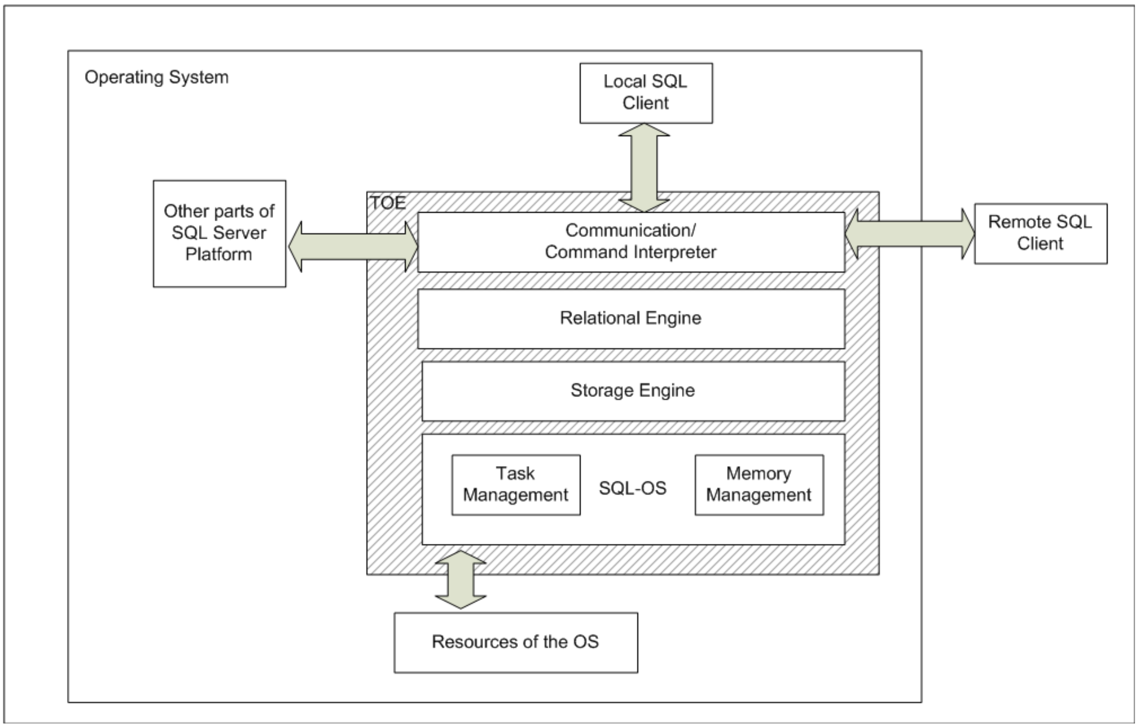


Figure 5-1: TOE Boundary

The following outlines each component.

[Communication/Command Interpreter]

The component that is responsible for communication processes with the outside of the TOE. All of SQL reception processes sent from external components such as clients and response processes to the outside are done through this component.

[Relational Engine]

The main component for database operation processes and security-related processes. This component interprets SQL statements received through Communication/Command Interpreter, performs the access right check, runs as an internal process to the database, and sends necessary responses.

[Storage Engine]

The component that manages the physical storage information, including the memory to store the databases and their related objects as well the HDDs. Necessary storage addresses and other information are passed based on demands from the Relational Engine.

[SQL-OS]

The component that manages various internal resources required for the TOE to run. This component is composed of two parts: Task Management that schedules the threads and Memory Management that manages memory resources used internally.

5.2 IT Environment

This TOE works on the hardware and operating system, processing SQL statements sent from clients via a network.

Part of the security functionality provided by the TOE is achieved by combining with the TOE itself and other functionality that is provided by the OS. The following are functionalities achieved by the functionality provided in the IT environment, or the OS:

- ID authentication functionality provided by Windows authentication
- Protection of the generated log data
- Date/time information to be used in the audit log

6 Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

SQL Server 2016 Database Engine Common Criteria Evaluation Guidance Addendum　Version 1.4 (2016-12-20)

SQL Server 2016 Database Engine Common Criteria Evaluation – SQL Server Books Online (2016-05-25)
(File name: SQL Server 2016 Technical Documentation.exe)

These documents are provided by downloading from the Website below. TOE users are required to refer to the following Website when purchasing the TOE.

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

7 Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

TÜV Informationstechnik GmbH, Evaluation Body for IT-Security that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2015-10 and concluded upon completion of the Evaluation Technical Report dated 2016-12. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, the evaluators directly visited the development and manufacturing sites on 2016-02 and examined procedural status conducted in relation to each work unit for configuration management, and delivery, by investigating records and interviewing staff. Further, the evaluators conducted checks of the developer testing and the evaluator testing by using the developer testing environment at the developer site from 2016-10 to 2016-12.

Concerns found in the evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility.

After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

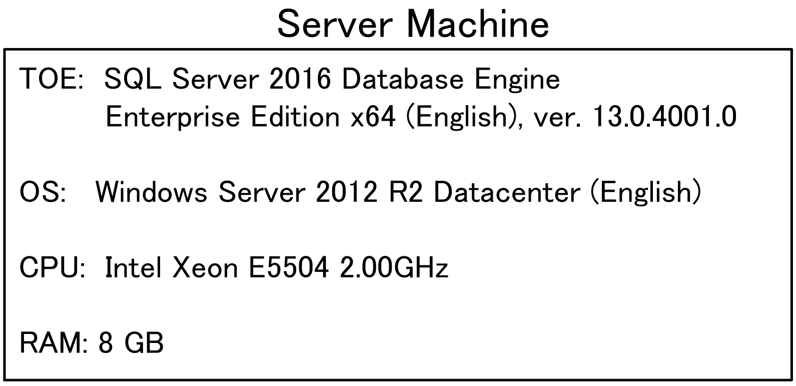
The evaluators confirmed the validity of the testing that the developer had conducted. As a result of the evidence obtained through the evaluation process and those confirmed validity, the evaluators conducted the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluators evaluated the integrity of the developer testing conducted by the developer and the documentation of actual testing results. The content of the developer testing evaluated by the evaluators is described as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration conducted by the developer.



Server Machine

TOE: SQL Server 2016 Database Engine
Enterprise Edition x64 (English), ver. 13.0.4001.0

OS: Windows Server 2012 R2 Datacenter (English)

CPU: Intel Xeon E5504 2.00GHz

RAM: 8 GB

Figure 7-1: Configuration of the Developer Testing

The developer testing was conducted in the same TOE testing environment as the TOE configuration identified by this ST.

2) Overview of the Developer Testing

This section outlines the overview of the developer testing.

a) Developer Testing Outline

The outline of the developer testing is shown below.

<Developer Testing Approach>

In the developer testing, SQL statements were sent to the clients' communication interface (the TOE's external interface), and the contents of the database reflected by the SQL operations as well as the response messages from the TOE (such as error messages) were observed.

In the actual testing, a combination of scripts (test scenarios) and a testing tool, developed by the developer to send a series of scripted SQL statements to the TOE and simultaneously automatically determine the result according to a verification method for the process result written out as a script, were used.

The validity of this testing tool and these test scenarios, including the design specification and integrity with applicable documents, was confirmed by the evaluators.

<Developer Testing Details>

In the developer testing, various scripts (test scenarios) were run using the above testing tool, and the contents of the test results determined (and output as test logs) by the tool based on the verification method written in the scripts were evaluated.

In some tests related to the access control functionality, multiple clients were connected and verified in a multi-session environment.

b) Scope of the Developer Testing Conducted

The developer testing was conducted by the developer for 185 scenarios. By the coverage analysis, it was verified that all security functionalities and external interfaces described in the functional specification had been tested.

c) Result

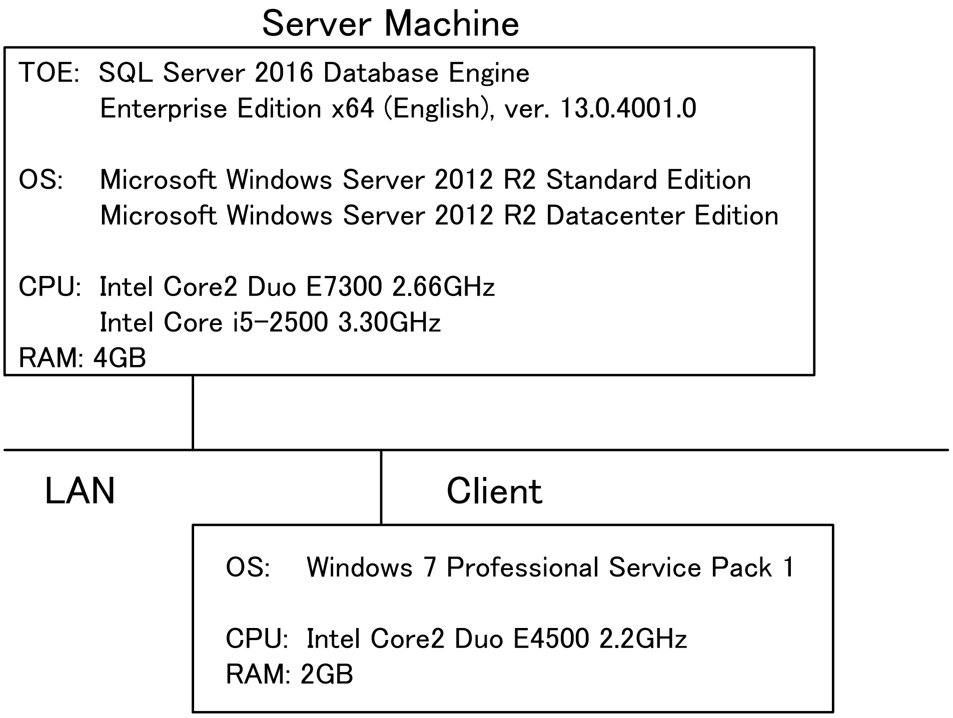
The evaluators confirmed an approach of the developer testing conducted and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach. The evaluators confirmed consistencies between the testing results expected by the developer and the actual testing results conducted by the developer.

7.4.2 Evaluator Independent Testing

The evaluators conducted a series of sample testing to reconfirm the execution of security functionalities by the test items extracted from the developer testing. In addition, the evaluators conducted the evaluator independent testing (hereinafter referred to as the "independent testing") to ensure that security functionalities are certainly implemented from the evidence obtained through the process of the evaluation. The independent testing conducted by the evaluators is explained as follows.

1) Independent Testing Environment

The configuration of the independent testing conducted by the evaluators is shown in Figure 7-2.



TOE: SQL Server 2016 Database Engine
Enterprise Edition x64 (English), ver. 13.0.4001.0

OS: Microsoft Windows Server 2012 R2 Standard Edition
Microsoft Windows Server 2012 R2 Datacenter Edition

CPU: Intel Core2 Duo E7300 2.66GHz
Intel Core i5-2500 3.30GHz
RAM: 4GB

OS: Windows 7 Professional Service Pack 1

CPU: Intel Core2 Duo E4500 2.2GHz
RAM: 2GB

Figure 7-2: Configuration of the Evaluator Independent Testing

As is the case with the developer testing, the independent testing was conducted in the same TOE testing environment as the TOE configuration identified by this ST. Note that a testing tool to send SQL statements is installed to the client machine.

2) Overview of the Independent Testing

This section outlines the overview of the independent testing conducted by the evaluators.

a) Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluators designed from the developer testing and the provided evaluation documentation are listed below.

<Viewpoints of the Independent Testing>

(1) To increase a variety of combinations of multiple operations related to security (account creation, right manipulation, database operation) and perform them as a series of processes.

(2) To use tools different from the developer testing tools to test the SQL transmission process to the TOE and the response reception process.

(3) To verify that the same results are obtained when the evaluators conduct all scenarios of the developer testing in order to confirm the validation of the developer testing.

b) Independent Testing Outline

This section explains the outline of the independent testing conducted by the evaluators.

<Independent Testing Approach / Method>

In the independent testing, a similar method as the developer testing was employed: a series of SQL statements were sent to the client communication interface, and the contents of the database with the SQL operations reflected as well as the response message from the TOE (such as error messages) were observed. To improve reliability by increasing variety in the testing environment, a test method other than the developer testing tool was employed.

<Independent Testing Tool>

“SqlCmd,” a command-line tool shipped with the TOE to perform various operations, including SQL transmission, was used in the independent testing, and the evaluators developed scripts to process a series of SQL processes.

<Independent Testing Details >

The independent testing was conducted by the evaluators for 12 scenarios. In the sampling test, all 185 of the developer testing scenarios were conducted. In addition, the evaluators conducted additional related tests (eight scenarios) to confirm that the TOE delivery and installation process and other processes can be performed as described in the applicable guidance.

Table 7-1 shows the viewpoints of the major independent testing conducted and their corresponding testing.

Table 7-1: Details of the Independent Testing Conducted

Viewpoint	Outline of the Independent Testing
(1) and (2)	- To verify that the access control is enforced in accordance with the defined right by performing a series of SQL statements to create new user accounts, set up the various default roles, define/set up new roles, create databases, and operate databases. Also, to verify that a series of audit logs are correctly generated. - By conducting normal and abnormal tests for the ID authentication functionality with two kinds of authentication methods provided by the TOE using different communication tools and different account settings, to verify that consistent results are obtained with the developer testing. - By increasing the variation of operations with the audit log capacity up to the limit, to verify that the same behavior listed in the specification is observed when resources are insufficient.

c) Result

All the independent testing conducted by the evaluators was correctly completed, and the evaluators confirmed the behavior of the TOE. The evaluators confirmed consistencies between the expected behaviors and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluators devised and conducted the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing conducted by the evaluators is explained as follows.

1) Overview of the Penetration Testing

An overview of the penetration testing conducted by the evaluators is as follows.

a) Vulnerability of Concern

The evaluators searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

(1) A brute-force attack may bypass the ID authentication functionality.

(2) Client requests with unauthorized formats and/or parameters may bypass the TOE security functionality.

(3) Unauthorized operations may bypass the security functionality due to existing vulnerabilities in the previous versions of the product that remain in this TOE.

(4) Illegally formatted data and special character codes used in ID authentication information may bypass the security functionality.

(5) Unauthorized access to the TOE may be possible from an unexpected network port interface.

(6) Unauthorized access to the protected assets may be possible by directly accessing the residual information on the memory and file systems.

b) Penetration Testing Outline

The evaluators conducted the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing was conducted in the same environment as the evaluator independent testing shown in Table 7-2.

Table 7-2 shows the main tools used in the penetration testing.

Table 7-2: Tools used in the Penetration Testing

Name (Version)	Outline
Metasploit (4.10.2)	Attack tool using vulnerability scanner and attack codes
nmap (7.31)	Port scan tool
ProcessExplorer (16.12)	Tool to collect process detail information provided by Microsoft
SqlCmd (13.1.811.168)	Command-line tool provided (along with SQL Server) by Microsoft
TCPView (3.05)	Investigation tool for network port and communication session provided by Microsoft

<Test items of the Penetration Testing Conducted>

Table 7-3 shows vulnerabilities of concern and the overview of the penetration testing corresponding to them. The evaluators conducted 12 penetration testing to determine the possibility of potentially exploitable vulnerabilities.

Table 7-3: Details of the Penetration Testing Conducted

Vulnerability	Penetration Testing Outline
(1)	To verify that the accounts with policy-based passwords have logically sufficient strength based on the measured duration and communication bandwidth when brute-force attacks are launched at these accounts, and that applicable policy is enforced to newly created accounts.
(2)	To verify that the TOE remains secure when a fuzzing test is performed against the execution format of the stored procedures managed by the TOE and usage parameters. To verify that the TOE's processes are protected by memory execution prohibition functionality that coordinates with the hardware and the OS, and that unauthorized operations to remove protection are prohibited.
(3)	To verify that no known vulnerability remains in this TOE by using Metasploit and related attack codes.
(4)	To verify that the TOE remains secure even when illegally formatted data and/or special character codes are used, by performing a fuzzing test for ID authentication information.
(5)	To verify that no unnecessary network ports are open by using the port scan tools and vulnerability scan tools. Also, to verify that unexpected network port control does not occur due to possible factors, including the TOE's start-up timing, by comparing the results obtained from multiple tools.
(6)	To verify by memory dump that there remains no residual information, which leads to unauthorized access, on the memory upon completion of the TOE execution process. Also, to verify that access control is enforced on the file systems in which the protected assets are stored.

c) Result

In the penetration testing conducted by the evaluators, the evaluators did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

In this evaluation, the configuration outlined in Figure 7-2 was evaluated. The TOE will not be used in the configuration which is significantly different from the above configuration components. Therefore, the evaluators determined the above evaluated configuration is appropriate.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:
  Base Protection Profile for Database Management Systems (DBMS PP), Version 2.07
- Security functional requirements: Common Criteria Part 2 Extended
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL2 package
- Additional assurance component ALC_FLR.2

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8 Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.
2. Contents pointed out in the Observation Reports shall properly be solved.
3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report, and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

TOE users shall be careful to see whether the restrictions and operational requirements of this TOE satisfy the actual TOE operational environment, by referring to the descriptions in "1.1.3 Disclaimers" and "4.2 Environmental Assumptions."

9 Annexes

There is no annex.

10 Security Target

The Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

SQL Server 2016 Database Engine Common Criteria Evaluation (EAL2+)
Security Target, Version 1.3, 2016-12-20, Microsoft Corporation

11 Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

SQL Structured Query Language; a database language to operate and define data for relational database.

SID Security Identifier; a unique identifier that is authorized to a user account or a group managed by Windows OS.

The definitions of terms used in this report are listed below.

System administrator A role assigned to users with authorized administrator role of the TOE. A system administrator is allowed for any operation related to security management and any operation for all databases.
When the TOE is installed, one system administrator account is always generated; however, another user could be authorized to have the system administrator right.

Stored procedure A series of operating procedures for databases is compiled as one program to store in the database management system.

12 Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001, (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002, (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003, (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004, (Japanese Version 1.0, November 2012)

[12] SQL Server 2016 Database Engine Common Criteria Evaluation (EAL2+) Security Target Version 1.3, 2016-12-20, Microsoft Corporation

[13] SQL Server 2016 Database Engine Evaluation Technical Report, Version 2, 2016-12-21, TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

[14] Base Protection Profile for Database Management Systems (DBMS PP), Version 2.07, September 9th, 2015