KECS-CR-11-63

# Chakra Max Core v2.0

# Certification Report

Certification No.: KECS-CISS-0355-2011

2011. 12. 29

IT Security Certification Center

| History of Creation and Revision | | | |
|---|---|---|---|
| No. | Date | Revised Pages | Description |
| 00 | 2011.12.29 | - | Certification report for Chakra Max Core v2.0<br>- First documentation |

This document is the certification report for Chakra Max Core v2.0 of Warevalley.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Laboratory (KTL)

# Table of Contents

# 1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of Chakra Max Core v2.0 from Warevalley Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is a database access control system, which is installed between DB clients, to protect DB, and in PCs of the DB client respectively, in order to perform access control and audit functions for a DB client who creates, changes, deletes, and retrieves data by connecting the protection target DB.

The TOE is situated in a safe environment protected by a firewall, and prevents unauthorized change, destruction, or leak of the protection target DB by controlling access to the protection DB as well as the access rights. In addition, the TOE provides the function that controls and monitors an authorized user’s access to the protection target DB, and manages the details involved in saving data modification and deletion, in order to prevent information misuse of a malicious internal DB client.

The TOE is composed of Chakra Max Server v2.0, Chakra Max Manager v2.0, and Chakra Max Client v2.0, which perform the following functions:

- Chakra Max Server v2.0: Performs access rights to the protection target DB and access control functions by analyzing packets, and provides the function of audit data generation and retrieval.
- Chakra Max Manager v2.0: Provides the GUI that enables the security manager to develop security management functions of the TOE.
- Chakra Max Client v2.0: Provides the routing function that allows DB clients to access the protection target DB in accordance with the TOE’s security policy, and the GUI for approval business.

The TOE can protect the following DBMS.

- Oracle 9i, 10g, 11g
- MySQL v4, v5
- MSSQL 2000, 2005, 2008
- Teradata v12
- DB2 UDB v8, v9
- Sybase ASE v12, v15
- Sybase IQ v12, v15
- Informix v10, v11

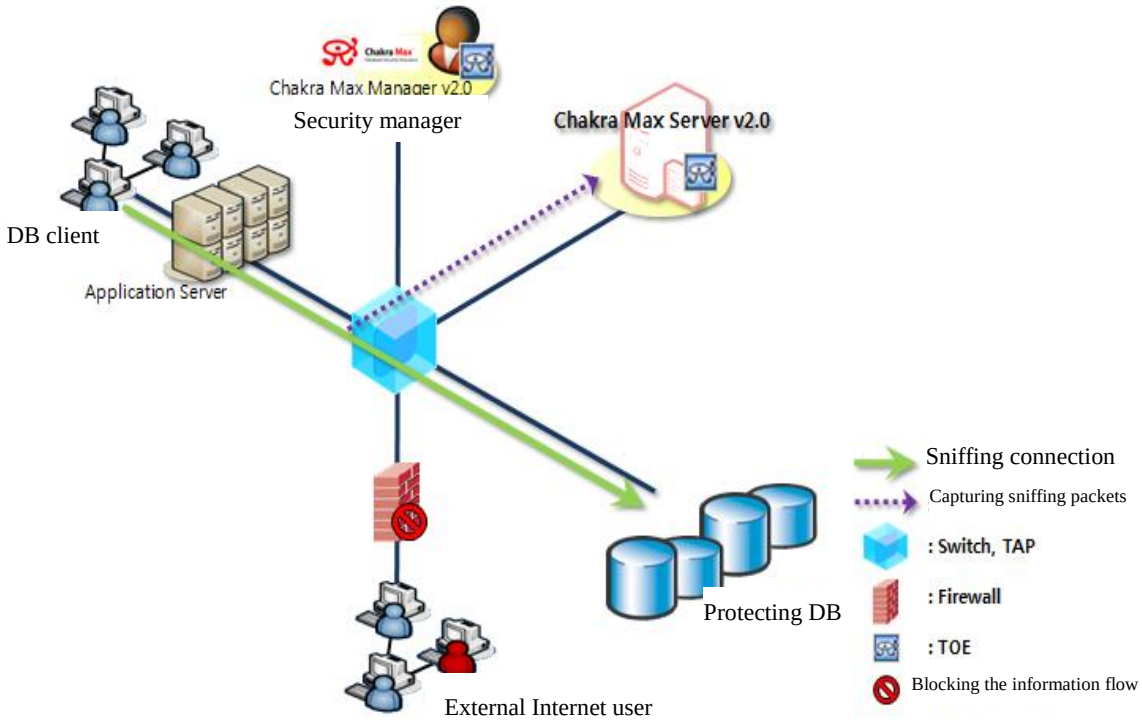
- Altibase v4, v5
- Tibero v3, v4

The evaluation of the TOE has been carried out by Korea Testing Laboratory (KTL) and completed on November 15, 2011. This report grounds on the evaluation technical report (ETR) KTL had submitted [5] and the Security Target (ST) [6].

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL4. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

The TOE can be composed of the sniffing mode, gateway mode, or the hybrid mode composed of both modes, as shown below.

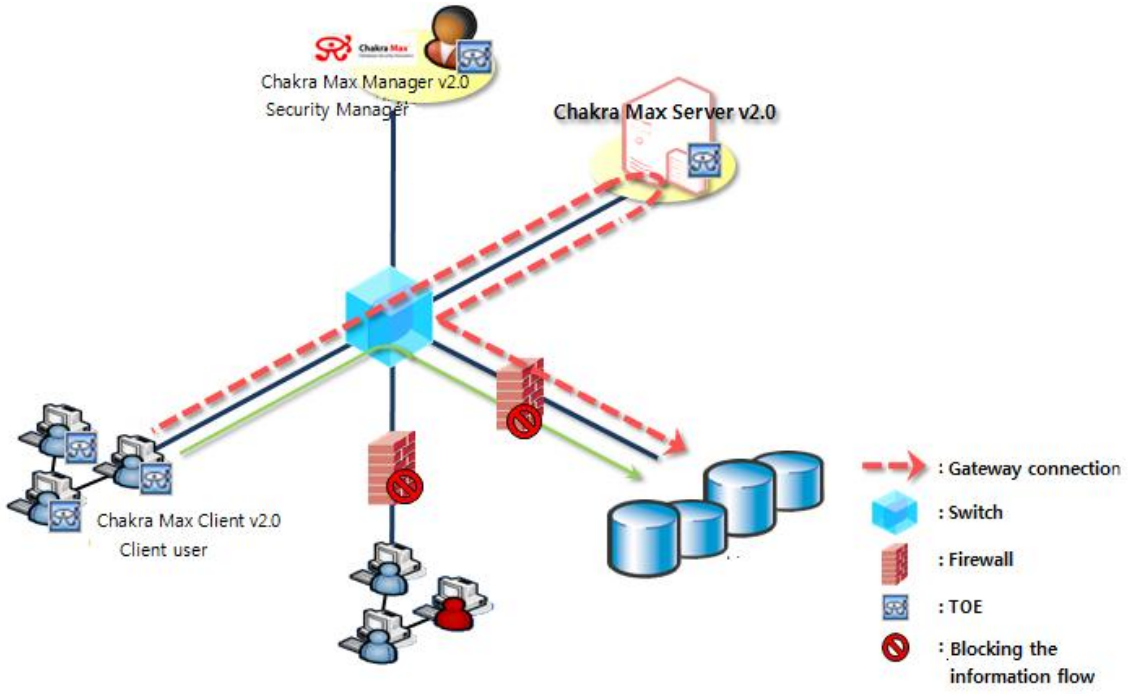
The TOE captures the packet from the network stream, using the switch or TAP that supports port mirroring. The TOE monitors and controls the formal SQL history of the application service, using the sniffing packet capture method as described above. The TOE can control the access of DB clients at the session level, and the security manager can block the session of an illegal DB access user.




[Figure 1] TOE Operational Environment (Sniffing Mode configuration)

In the gateway mode, the TOE routes the packets of security client users, and prohibits them from accessing the protection target DB directly. Therefore, every access of the security client user to the protection target DB passes through the TOE. Using this configuration, the TOE can control DB client access at the session and SQL level, and the security manager can block the session and SQL of any security client user that shows illegal behavior in real time.

The DB connection session of a PC not installed with Chakra Max Client v2.0 or not running the service will be blocked by the firewall in the gateway mode.

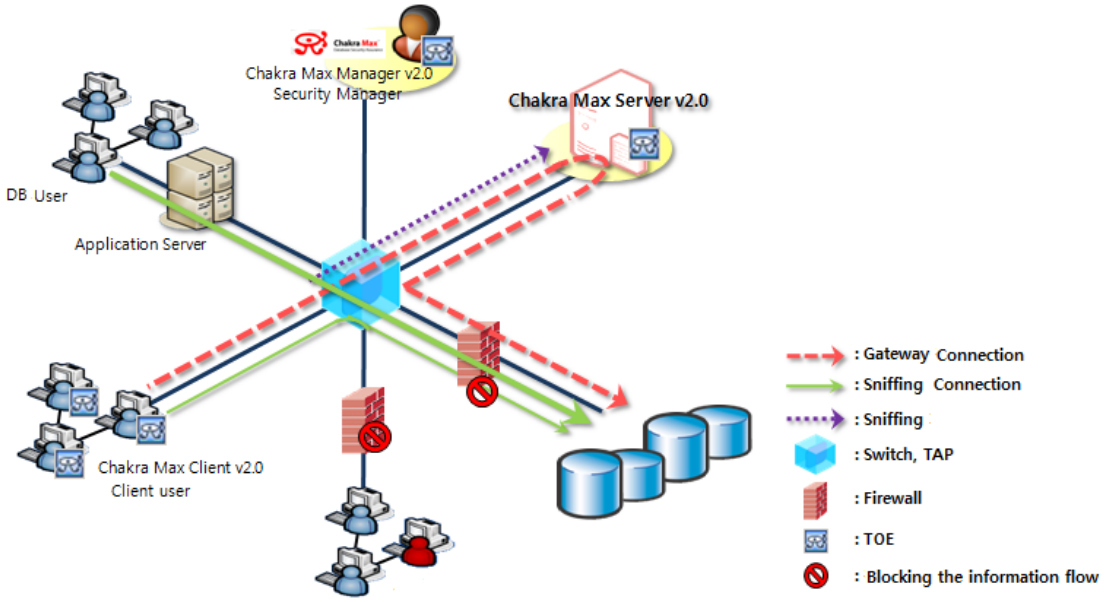



[Figure 2] TOE Operational Environment (Gateway Mode Configuration)

The TOE can also be configured in a hybrid mode, which runs the sniffing and gateway modes at the same time. Every DB client's access to the protection target DB, including the security client user group, will be logged, controlled, audited, and managed in an integrated manner.

The network environment in the hybrid mode should be configured in such a way that the firewall installed before the protection target DB should block direct TOE access of the security client user, and only the allowed application server can perform a sniffing connection. In addition, the user groups running in the sniffing mode and gateway mode should be clearly separated, and the network should be configured safely so that

the packets sent by each operation mode are not mixed with each other.




[Figure 3] TOE Operational Environment (Hybrid Mode configuration)

**Certification Validity**: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

# 2. Identification

The TOE is product package consisting of the following components and related guidance documents.

| Type | Identifier | Release | Delivery Form |
|---|---|---|---|
| SW | Chakra Max Server | V2.0.0 | Setup File |
| | Chakra Max Manager | V2.0.0 | |
| | Chakra Max Client | V2.0.0 | |
| DOC | Chakra Max Core v2.0 User Manual | v1.3 | Softcopy |

| Type | Identifier | Release | Delivery Form |
|---|---|---|---|
| | Chakra Max Core Administrator Manual | v1.3 | |

[Table 1] TOE identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

| | |
|---|---|
| Scheme | Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009)<br>Korea Evaluation and Certification Regulation for IT Security (July 20, 2011) |
| TOE | Chakra Max Core v2.0 |
| Common Criteria | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009 |
| EAL | EAL4 |
| Developer | Warevalley Co., Ltd. |
| Sponsor | Warevalley Co., Ltd. |
| Evaluation Facility | Korea Testing Laboratory (KTL) |
| Completion Date of Evaluation | November 15, 2011 |
| Certification Body | IT Security Certification Center |

[Table 2] Additional identification information

# 3. Security Policy

The TOE complies security policies defined in the ST [6] by security objectives and security requirements. The TOE provides security features to identify and authenticate authorized users, to generate audit records of the auditable events, and to securely manage the TOE functionality and authorized user accounts information.
For more details refer to the ST [6].

# 4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [6], chapter 3.3):

- The TOE is installed in the environment where the intranet is securely maintained by way of the network setting like firewall so that it is located in the physically safe environment only a Security Administrator may access.
- A Security Administrator in the TOE is well trained about the TOE management function and performs the management task in a correct and benign way according to the guidelines of, administrator.
- An administrator of TOE performs the task of removing all the unnecessary services or methods in the operating system and strengthening the vulnerabilities in the operating system to guarantee the credibility and stability of the operating system of a server in which TOE is operated.
- The TOE operation environment provides a reliable repository which saves the audit record. Repository may not be created, modified or deleted without the request of the TOE.
- Mail Server and SMS Server for the email or SMS sending functions provided by TOE are located in the physically secured environment.
- A Security Administrator creates SSL authentication certificate to be used in SSL communication in the encrypted communication used for TSF data transfer before the first operation after the TOE installation, and the cerficate is managed safely.
- Since data communication channel between the separated TOEs are transferred while encrypted through SSL, the security from leaking out is guaranteed.
- The TOE is provided with reliable Time-stamp via a trusted administrator..
- In the TOE, the firewall is installed at the front end of all the Protective DBs in a Gateway Mode and Hybrid Mode environment so that the environment is provided in which every DB user may be forced to access the Protective DB only through the TOE.
- The TOE may monitor all the details about access to the Protective DB..

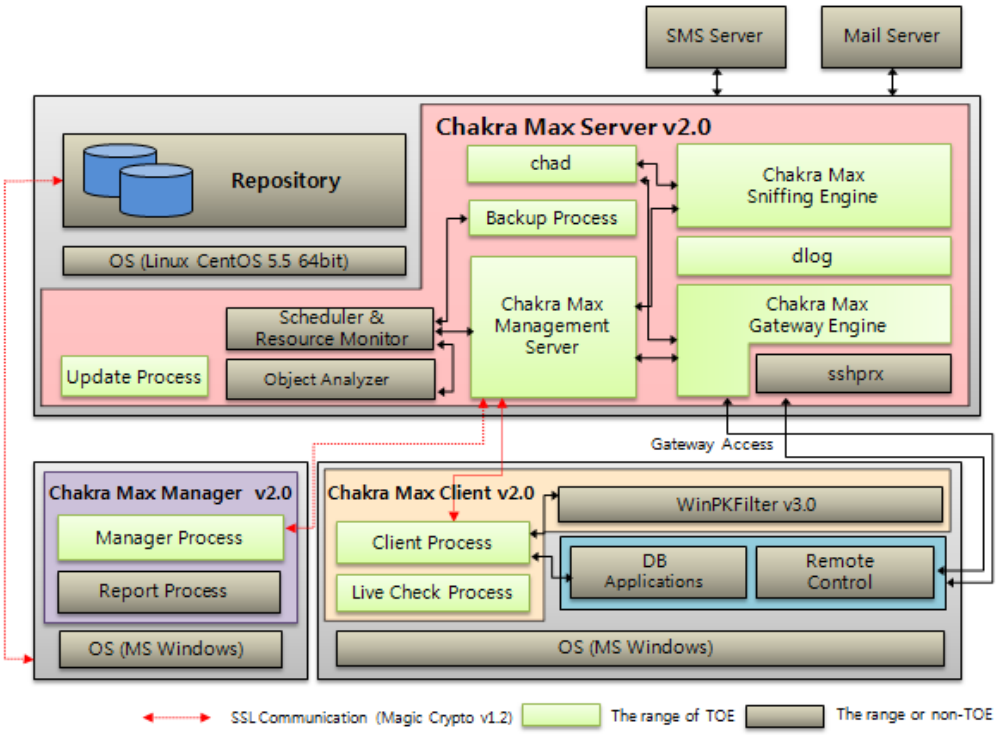
It is assumed that the TOE is installed and operated based on the following hardware and operating system.

| TOE Component | Recommended Specifications | |
|---|---|---|
| | Hardware | Software/Firmware |
| Chakra Max Server v2.0 | CPU: Dual Core 2.0Ghz Xeon CPU (64bit) * 2 ea. or more<br>RAM: 4GB Main Memory or more<br>NIC: 10/100/1000Mb NIC 3 ea. or more<br>HDD: 80GB or more | Linux CentOS v5.5 (Kernel 2.6.18)<br>MySQL v5.0 |
| Chakra Max Manager v2.0 | CPU: Pentium P4 1.5GHz or faster<br>RAM: 1GB or more<br>NIC: 10/100/1000Mb NIC 1 ea. or more<br>HDD: 600 MB ore more | MS Windows 2000/XP/2003/2005/Vista/7 |
| Chakra Max Client v2.0 | CPU: Pentium P4 1.5GHz or faster<br>RAM: 512MB or more<br>NIC: 10/100/1000Mb NIC 1 ea. or more<br>HDD: 600 MB or more | MS Windows 2000/XP/2003/2005/Vista/7 |

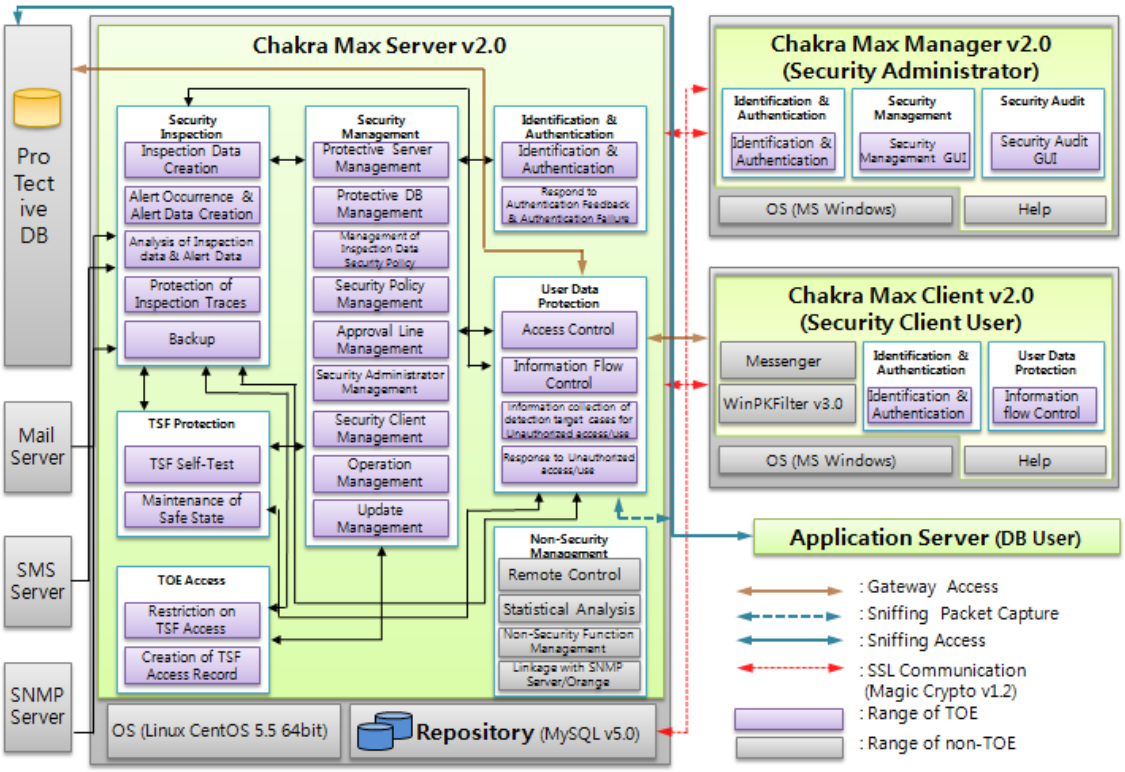
[Table 3] Required non-TOE Hardware and OS

# 5. Architectural Information

[Figure 4] and [Figure 5] show architectural information and the logical scope of the TOE.




[Figure 4] Architectural Information of the TOE




[Figure 5] Logical boundary of the TOE

**Chakra Max Server v2.0**

- Chakra Max Management Server

It communicates with Chakra Max Sniffing Engine and Chakra Max Gateway Engine in real-time, and applies security policy so as to help with the access control to Protective DB and the information flow control. In addition, it operates the license management function. Also, in case of MySQL v5.0 disruption/error, it operates a function of saving the audit data temporarily saved in the file system normally into MySQL v5.0 after MySQL v5.0 gets back to the normal state.

And it communicates with Chakra Max Manager v2.0 and Chakra Max Client v2.0 in real time, and apply the security policy or settings made through GUI of Chakra Max Manager v2.0. Also, it synchronizes time of Chakra Max Manager v2.0 and Chakra Max Client v2.0 with that of Chakra Max Server v2.0 to provide reliable time display.

- Chakra Max Sniffing Engine

It is a process of controlling and monitorning the session in which DB users access to Sniffing. It is utilized as a target of monitoring formatted SQL which access through application.

- Chakra Max Gateway Engine

It is a process of controlling and monitoring a Gateway acess session of a Security Client User. After deciding whether or not it applies session information, SQL information, or security policy, it notifies Chakra Max Client v2.0 of its decision, applies a security policy to result values in the Protective DB and delivers them to Security Client User.

- Backup Process

This process backs up the audit data and security setting data of repository periodically or manually and if necessary it recovers them to be available for query.

- chad

It is a daemon process in which the conditions of Chakra Max Server v2.0 are checked and controlled.

**Chakra Max Manager v2.0**

- Manager Process

It executes Chakra Max Manager v2.0 programs, communicates with Chakra Max Server v2.0 and plays a role in delivering the history and data of security management an administrator implemented to Chakra Max Server v2.0.

**Chakra Max Client v2.0**

- Client Process

It executes Chakra Max Client v2.0 programs, communicates with Chakra Max Server v2.0 and plays a role in routing all data the Protective DB sends and receives via Chakra Max Server v2.0.

- Live Check Process

It judges whether or not Client Process has been executed; if Client Process stops, it plays a role clearing Network Driver such as the routing information converted for operation in a Gateway Mode.

# 6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

| Identifier | Release | Date |
|---|---|---|
| Chakra Max Core v2.0 Administrator Manual | v1.3 | August 3, 2011 |
| Chakra Max Core v2.0 User Manual | v1.3 | August 3, 2011 |

[Table 4] Documentation

# 7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. The developer's tests were performed on each distinct operational environment of the TOE (see chapter 1 of this report for details about operational environment of the TOE).

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined in the functional specification, and demonstrated that the TSF behaves as described in the functional specification.

The developer tested subsystems including their interactions, and analyzed testing results according to the assurance component ATE_DPT.1.

Therefore the developer tested all SFRs defined in the ST [6].

The evaluator performed all the developer’s tests (a total of 233 tests), and conducted a total of 22 independent testing based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [7]. The evaluator considered followings when devising a test subset:

- TOE security functionality: The TOE protects DB, and in PCs of the DB client respectively, in order to perform access control and audit functions for a DB client. the function that controls and monitors an authorized user’s access to the protection target DB, and manages the details involved in saving data modification and deletion, in order to prevent information misuse of a malicious internal DB client, and
- Developer's testing evidence: The evaluator analyzed evaluation deliverables for ATE_COV.2, ATE_DPT.1, and ATE_FUN.1 to understand behavior of the TOE security functionality and to select the subset of the interfaces to be tested, and
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL4, and the evaluator tried to balance time and effort of evaluator's activities between EAL4 assurance components.

Also, the evaluator conducted a total of 38 penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, weak cryptography, flaws in networking protocol implementation, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

# 8. Evaluated Configuration

The TOE is Chakra Max Core v2.0. The TOE is product package which is consisting of following components:

- Chakra Max Server v2.0.0
- Chakra Max Manager v2.0.0
- Chakra Max Client v2.0.0

The TOE is identified by each TOE component name and version number including release number. The TOE identification information is provided GUI or CLI according to the TOE component (or both of them).
And the guidance documents listed in this report chapter 6, [Table 3] were evaluated with the TOE.
The TOE can be installed and operated in a three different type of networking environment (i.e., Sniffing Mode Type, Gate Mode Type, and Hybrid Mode Type), refer to chapter 1 of this report for details about operational environment of the TOE.

# 9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL4.

## 9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.
The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.
The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.
The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.
The ST doesn't define any extended component. Therefore the verdict PASS is assigned to ASE_ECD.1.
The Security Requirements is defined clearly and unambiguously, and it is internally

consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.
The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.
Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation.
The verdict PASS is assigned to the assurance class ASE.

## 9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.
The developer uses a CM system that uniquely identifies all configuration items, and the ability to modify these items is properly controlled. Therefore the verdict PASS is assigned to ALC_CMC.4.
The configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.4.
The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Therefore the verdict PASS is assigned to ALC_DVS.1.
The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.
The evaluator shall examine the development tool documentation provided to determine that each development tools is well-defined. Therefore the verdict PASS is assigned to ALC_TAT.1
Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, and the delivery activity.
The verdict PASS is assigned to the assurance class ALC.

## 9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

## 9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. It provides a detailed description of the SFR-enforcing subsystems and enough information about the SFR-supporting and SFR-non-interfering subsystems for the evaluator to determine that the SFRs are completely and accurately implemented. Therefore the verdict PASS is assigned to ADV_TDS.3.

The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, the actions, results and error messages of each TSFI are also described sufficiently that it can be determined whether they are SFR-enforcing, with the SFR-enforcing TSFI being described in more detail than other TSFIs. Therefore the verdict PASS is assigned to ADV_FSP.4.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

The developer has provided the implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions. The implementation representation is in the form used by development personnel and the mapping between the TOE design description and the sample of the implementation representation to determine that it is accurate. Therefore the verdict PASS is assigned to ADV_IMP.1.

Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), and a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

## 9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.
The developer has tested the TSF subsystems against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.1.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

## 9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing Enhanced Basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.3.
Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t

allow attackers possessing Basic attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

## 9.7 Evaluation Result Summary

| Assurance Class | Assurance Component | Evaluator Action Elements | Verdict | | |
|---|---|---|---|---|---|
| | | | Evaluator Action Elements | Assurance Component | Assurance Class |
| ASE | ASE_INT.1 | ASE_INT.1.1E | PASS | PASS | PASS |
| | | ASE_INT.1.2E | PASS | | |
| | ASE_CCL.1 | ASE_CCL.1.1E | PASS | PASS | |
| | ASE_SPD.1 | ASE_SPD.1.1E | PASS | PASS | |
| | ASE_OBJ.2 | ASE_OBJ.2.1E | PASS | PASS | |
| | ASE_ECD.1 | ASE_ECD.1.1E | PASS | PASS | |
| | | ASE_ECD.1.2E | PASS | | |
| | ASE_REQ.2 | ASE_REQ.2.1E | PASS | PASS | |
| | ASE_TSS.1 | ASE_TSS.1.1E | PASS | PASS | |
| | | ASE_TSS.1.2E | PASS | | |
| ALC | ALC_LCD.1 | ALC_LCD.1.1E | PASS | PASS | PASS |
| | ALC_CMS.3 | ALC_CMS.4.1E | PASS | PASS | |
| | ALC_CMC.3 | ALC_CMC.4.1E | PASS | PASS | |
| | ALC_DVS.1 | ALC_DVS.1.1E | PASS | PASS | |
| | | ALC_DVS.1.2E | PASS | | |
| | ALC_DEL.1 | ALC_DEL.1.1E | PASS | PASS | |
| | ALC_TAT.1 | ALC_TAT.1.1.E | PASS | PASS | |
| AGD | AGD_PRE.1 | AGD_PRE.1.1E | PASS | PASS | PASS |
| | | AGD_PRE.1.2E | PASS | PASS | |
| | AGD_OPE.1 | AGD_OPE.1.1E | PASS | PASS | |
| ADV | ADV_TDS.3 | ADV_TDS.3.1E | PASS | PASS | PASS |
| | | ADV_TDS.3.2E | PASS | PASS | |
| | ADV_FSP.4 | ADV_FSP.4.1E | PASS | PASS | |
| | | ADV_FSP.4.2E | PASS | | |
| | ADV_ARC.1 | ADV_ARC.1.1E | PASS | PASS | |

| Assurance Class | Assurance Component | Evaluator Action Elements | Verdict | | |
|---|---|---|---|---|---|
| | | | Evaluator Action Elements | Assurance Component | Assurance Class |
| | ADV_IMP.1 | ADV_IMP.1.1E | PASS | PASS | |
| ATE | ATE_COV.2 | ATE_COV.2.1E | PASS | PASS | PASS |
| | ATE_DPT.1 | ATE_DPT.1.1E | PASS | PASS | |
| | ATE_FUN.1 | ATE_FUN.1.1E | PASS | PASS | |
| | ATE_IND.2 | ATE_IND.2.1E | PASS | PASS | |
| | | ATE_IND.2.2E | PASS | | |
| | | ATE_IND.2.3E | PASS | | |
| AVA | AVA_VAN.3 | AVA_VAN.3.1E | PASS | PASS | PASS |
| | | AVA_VAN.3.2E | PASS | | |
| | | AVA_VAN.3.3E | PASS | | |
| | | AVA_VAN.3.4E | PASS | | |

[Table 5] Evaluation Result Summary

# 10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- Various methods can be used to configure the authentication policies, the access control policies and the warning policies for the DB query used in the evaluated TOE, so users should receive proper education on how to operate the product before and after its installation, by considering the DB characteristics.
- If there is insufficient audit data storage space and the limit is exceeded, TOE will notify the manager via email and start overwriting the oldest data, but the manager should be responsible for acquiring sufficient monitoring data storage by consistently audit the storage space.
- The evaluated TOE can be organized in Gateway Mode, Sniffing Mode or Hybrid Mode depending on how the DB server and the network are

implemented. The manager should select the appropriate operation mode for the operating environment. In addition, the manager should implement the network environment such that TOE can safely protect the protection target DB against attacks.

- The evaluated TOE is comprised of Chakra Max Server v2.0, Chakra Max Manager v2.0 and Chakra Max Client v2.0, and to ensure safe communication among them, a private certificate for SSL communication is required. Only one certificate should exist for the entire product, which should be managed by an authorized manager.
- Of the various TOE operation modes, sniffing mode does not support efficient real-time blocking when a DB user's access to the protection target DB server is blocked. For this reason, if the operation mode is set to sniffing mode, then the manager should be notified of the fact. We recommend that you use gateway mode if you want to maximize the security of the protection target DB and the effectiveness of the DB access control function.

# 11. Security Target

The Chakra Max Core v2.0 Security Target v1.8, July 4, 2011 [6] is included in this report by reference.

# 12. Acronyms and Glossary

| | |
|---|---|
| CC | Common Criteria |
| DBMS | Database Management System |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| IETF | Internet Engineering Task Force |
| LDAP | Lightweight Directory Access Protocol |
| PP | Protection Profile |
| RFC | Request For Comments |
| SAR | Security Assurance Requirement |
| SFR | Security Functional Requirement |

| | |
|---|---|
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |

| | |
|---|---|
| DB user (Database Client) | This refers to a user who accesses the protection target DB server managed by TOE, using the database client program. It refers to either DBA, developer, DB operator, or application server that performs DB works by using SQL of DCL, DDL, or DML with the database client program. |
| NAT(Network Address Transfer) | When a DB user's handset accesses the protection target DB server, the DB IP address inside the packet is changed to the Proxy Gateway IP address to change the target of packet delivery. A handset on which the module providing the NAT function is installed sets up a DB user's access to the DB server automatically via the proxy gateway so that every packet is controlled. |
| Passive | This refers to the passive receipt of packets without taking any action on the network. |
| Port Mirroring | Monitoring packets on the network.. |
| Sniffing | Reading in the packet data transmitted over a communication network. (mostly used for monitoring purposes). |
| SQL(Structured Query Language) | Language made to access the database. |
| TAP(Test Access Point) | Passive-type device that can perform permanent monitoring and analysis without affecting the data flows over the network. |

# 13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-004, July 2009

[3] Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009)

[4] Korea Evaluation and Certification Regulation for IT Security (July 20, 2011)

[5] Chakra Max Core v2.0 Evaluation Technical Report V1.10, November 15, 2011

[6] Chakra Max Core v2.0 Security Target v1.8, July 4, 2011