Security Target v1.8

Chakra Max Core v2.0

2011.07.04

Document Information

Project Title	CC certified		
Project Manager	Park, Jong-sung	Version	v1.8
Project Stage		Execution Date	2010.05.17
Name Of Creator	Lee, Hye-jin	Date of Last Update	2011.07.04

Updated Contents

Date Of Update	Updated Contents	Updated By	Version
2010.05.17	Initial Release	Lee, Hye-jin	v1.0
2010.06.07	Changed from CC V3.1 r2 to r3	Lee, Hye-jin	v1.1
2010.07.06	Requirements for security functions updated	Lee, Hye-jin	v1.2
2010.08.17	TOE details updated	Lee, Hye-jin	v1.3
2010.10.27	TOE summary specifications written	Lee, Hye-jin	v1.4
2010.11.04	Protective DB added	Lee, Hye-jin	v1.5
2010.11.15	Requirements for security functions	Lee, Hye-jin	v1.6
2011.01.11	OR Requirements for update applied	Lee, Hye-jin	v1.7
2011.07.04	OR Requirements for update applied	Lee, Hye-jin	v1.8

TABLE OF CONTENTS

1 Introduction to ST

This ST identifies the security function and the assurance means of Chakra Max Core v2.0 (Chakra Max Server v2.0, Chakra Max Manager v2.0, and Chakra Max Client v2.0 included.), and describes the conformance of CC.

This ST consists of the following chapters.

- Chapter 1 is an introduction to ST, which describes the ST and TOE reference, TOE overview, TOE description, the rules for writing specification and the definition of terms.

- Chapter 2 contains the contents of Conformance claims, which claims the conformance to CC, protection profile and package and specifies the ways to decide the validity of Conformance claims and claim conformance to protection profile

- Chapter 3 is a definition of security problems, which defines security problems such as the threats to be dealt with in TOE and TOE operating environment, organizational security policy (OSP), and the assumptions regarding TOE operating environment.

- Chapter 4 suggests the security target and relevant rationale of TOE and operating environment.

- Chapter 5 deals with the definition of expanded component and specifies the newly defined requirements based on the expanded component, not based on CC.

- Chapter 6 is security requirements, which describes the security functional requirements and the security assurance requirements and suggests the theoretical ground for them.

- Chapter 7 is a TOE summary specification, which summarizes and specifies TOE functions and describes the ways for TOE to meet the security functional requirements.

1.1 Reference to ST

It provides information required for identifying and controlling ST uniquely. The reference information of this ST is as follows:

ST Title	Chakra Max Core v2.0 Security Target v1.8
ST Version	v1.8
Date of writing	4th July 2011
Writer	Authentication team in Quality management office of WareValley, Co., Ltd.
CC version	CC V3.1r3 (Notification no. 2009-52 of Ministry of Public Administration and Safety)
Relevant protection profile	N/A
Key words	DB security, DB access control, access control, access control, audit, approval

1.2 TOE reference

TOE information that this ST identifies uniquely is as follows

Product Name	Chakra Max v2.0
TOE identifier	Chakra Max Core v2.0
TOE version	v2.0
Developer	WareValley Lab. Co., Ltd.

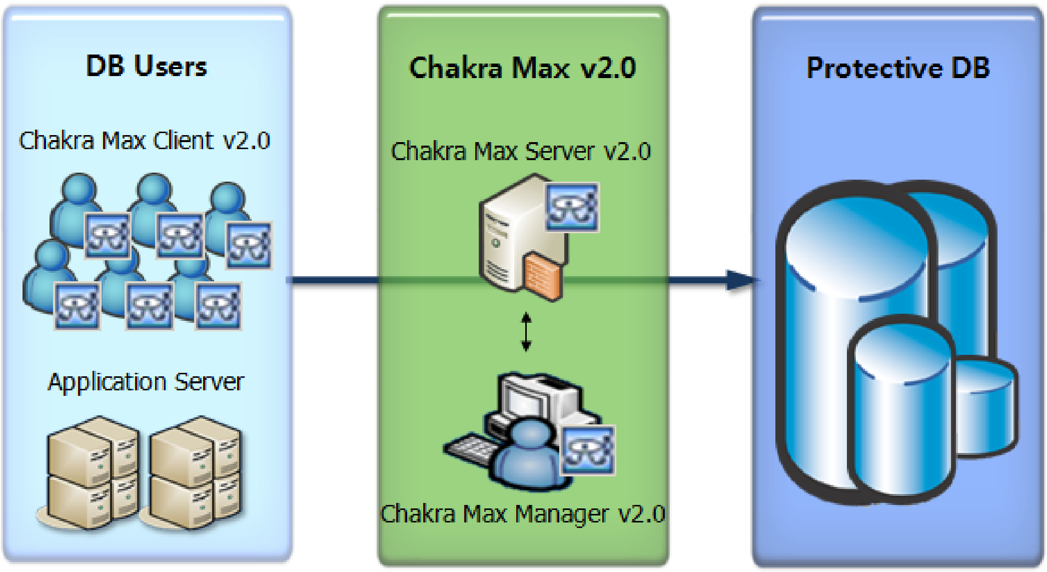
1.3 TOE Overview

It describes uses, main security characteristics, product types and the range of TOE and identifies hardware/software/firmware required in TOE which correspond to non-TOE.

1.3.1 Uses and main security characteristics of TOE

TOE is Chakra Max Core v2.0 by WareValley Co., Ltd. TOE is a DB access control system that is logically installed in between DB user and Protective DB and PCs of DB users respectively to carry out the function of access control and audit for DB users who connect with Protective DB for creating, updating, deleting and querrying data.

TOE is located in the safe environment which is protected as the firewall system and prevents the unauthorized change, destruction and leak in Protective DB by controlling the access and privilege to DB. Also, TOE provides the functions of monitoring the access of DB users to the Protective DB and the audit as well as the function of managing details about change and deletion of saved data. By doing so, it prevents the information misuse by internal DB users for malicious purposes.



[Figure 1-1] TOE configuration environment

TOE is divided into Chakra Max Server v2.0, Chakra Max Manager v2.0, and Chakra Max Client v2.0, and each part carries out the roles as follows:

- Chakra Max Server v2.0: It analyzes the packet to operate the function of controlling the privilege of access to Protective DB, controls the connection to the DB, create the audit data and provides the query function.
- Chakra Max Manager v2.0: It provides GUI on which a Security Administrator can operate a function of security management for TOE.
- Chakra Max Client v2.0: It provides the routing function by which a DB user can access the Protective DB according to the security policy of TOE and provides the GUI on which he can make approval.

The characterstics of security function that TOE provides are as follows:

- security audit
- user data protection
- identification and authentication
- security management
- TSF protection
- TOE access

The kinds of DBMS that TOE protects are as follows:

- 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

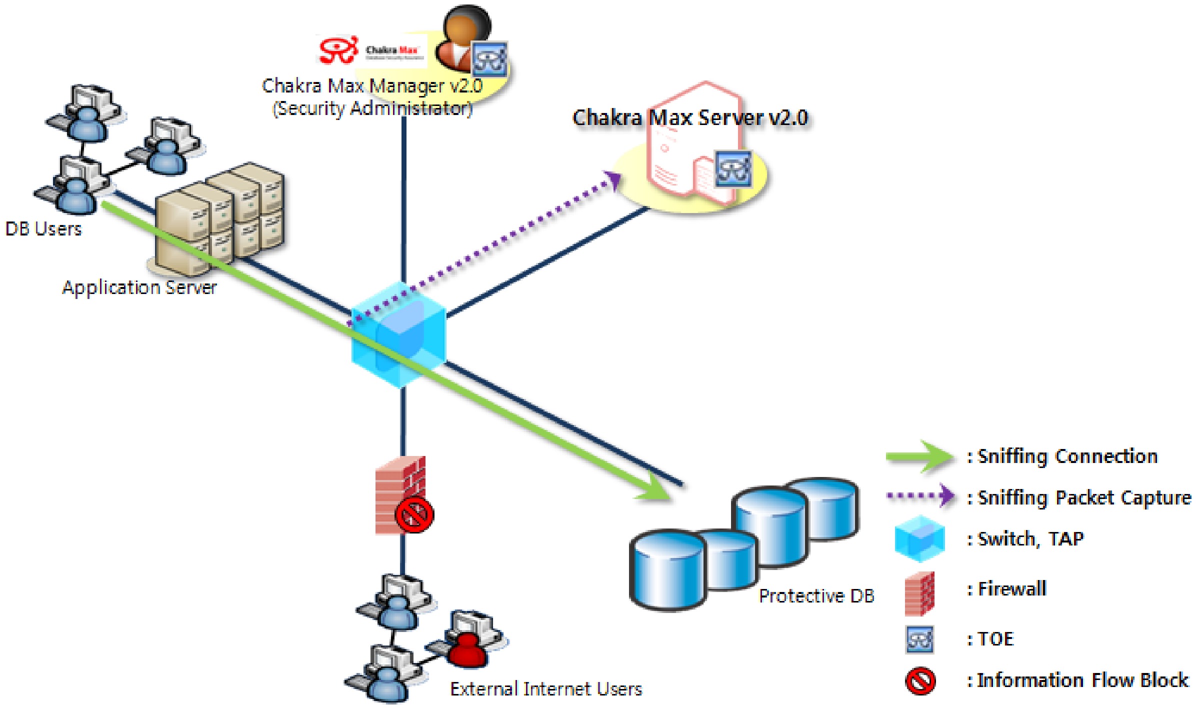
1.3.2 TOE Type

TOE is a DB access control system in which the functions of logging, control, audit and management of the access to the Protective DB are given.

Among the systems that form TOE, Chakra Max Server v2.0, which operates a security function, is composed in the network stream between DB users and the Protective DB when in operation. And Chakra Max Manager v2.0, which provides a security management interface, is installed in Security Administrator's PC. Chakra Max Client v2.0, which routes the access to the Protective DB using Gateway mode, is installed to DB users' PC in operation. DB users are to be classified into the group which make Sniffing access through Application Server, etc. and a Security Client User group, which make a Gateway acess via TOE. Chakra Max Client v2.0 is installed and operated only in Security Client User's PC.

TOE can be composed of a Sniffing Mode and a Gateway Mode as below. It can also be configured as a Hybrid Mode that comprises both modes altogether.

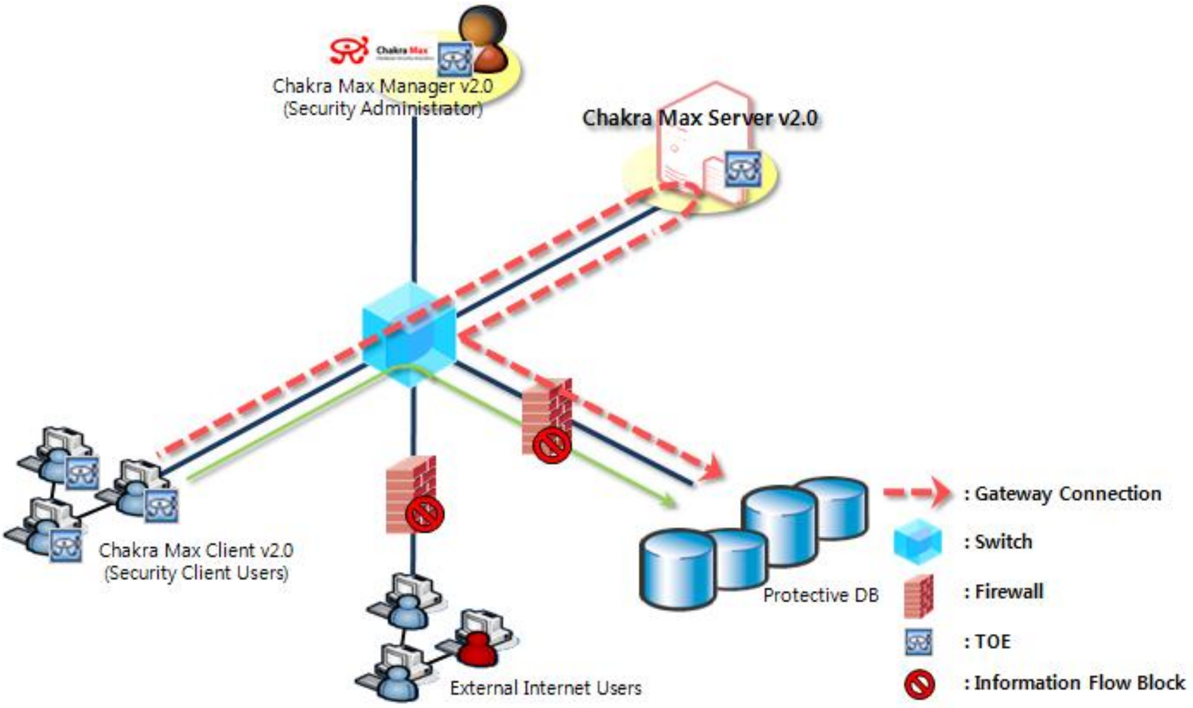
Roughly speaking, a sniffing Mode is configured as in the figure below.



[Figure 1-2] Sniffing Mode Configuration

TOE captures the packets in the network stream through TAP or switch that supports Port Mirroring. Through the Sniffing packet capture mode like this, TOE can monitor and control the formatted record of SQL which is operated through Application Server. In a Sniffing Mode, TOE can control access of DB users by session unit and a Security Administrator is able to block the session for unauthorized access of DB users in real-time.

A Gateway Mode is configured roughly as in the figure below.



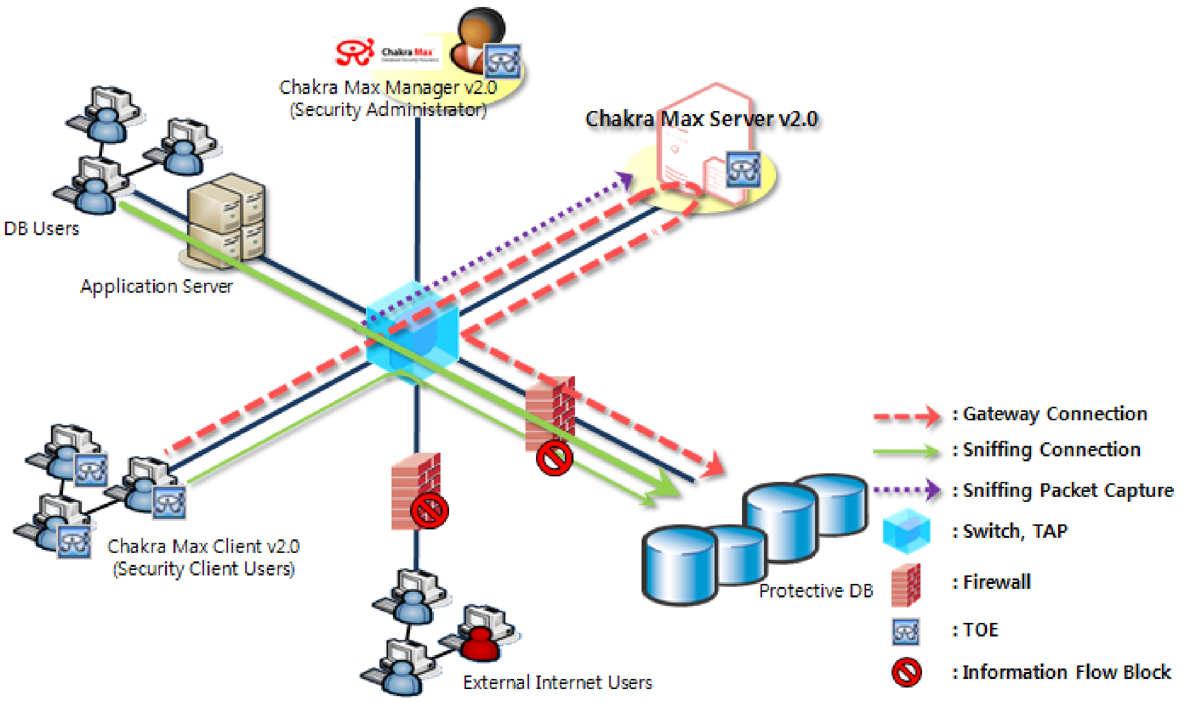
[Figure 1-3] Gateway Mode Configuration

In a Gateway Mode, TOE routes the packets of Security Client Users to itself (TOE) and prevents Security Client Users from gaining a direct access to the Protective DB. Therefore, access of Security Client Users to the Protective DB will be routed via TOE. In this configuration, TOE can control the access of DB users by session unit or SQL unit and a Security Administrator can block the session or SQL of Security Client Users who show an unauthorized behavior in real time.

In a Gateway Mode, if Chakra Max Client v2.0 is not installed, or if a session accesses the DB from a PC which did not execute the service, it will be blocked by IT environments such as firewall, etc.

Also TOE can be configured in a Hybrid Mode. In this configuration, a Sniffing Mode and a Gateway Mode are operated at the same time. So, access to the Protective DB by all DB users including a Security Client User group is integrally admnistered by logging, control, audit, or management.

A Hybrid Mode is configured roughly as in the figure below.



[Figure 1-4] Hybrid Mode Configuration

1.3.3 Hardware/Software/Firmware required in TOE

The minimum hardware/software requirements for TOE operation is as follows:

[Table 1-1] HW/SW operating environment

TOE	Environment	
	Hardware	Software/Firmware
Chakra Max Server v2.0	CPU: Dual Core 2.0Ghz Xeon CPU(64bit)* 2EA or higher RAM: 4GB Main Memory or higher NIC: 10/100/1000Mb NIC 3EA or higher HDD: 80GB or more capacity	Linux CentOS v5.5 (Kernel 2.6.18) MySQL v5.0
Chakra Max Manager v2.0	CPU: Pentium P4 1.5GHz or higher RAM: 1GB or higher NIC: 10/100/1000Mb NIC 1EA or higher HDD: 600 MB or more	MS Windows 2000/XP/2003/2005/Vista/7
Chakra Max Client v2.0	CPU: Pentium P4 1.5GHz or higher	MS Windows

	RAM: 512MB or higher NIC: 10/100/1000Mb NIC 1EA or higher HDD: 600 MB or more capacity	2000/XP/2003/2005/Vista/7

TOE is a Repository which uses File System of MySQL v5.0 and Linux CentOS v5.5.stem. File System saves the log of all processes in Chakra Max Server v2.0 and plays a role of saving the Backup file of audit data. MySQL v5.0 is used for saving audit data and alert data of TOE and TSF data.

Also, when MySQL v5.0 is installed, the environment should be set up so that the encrypted communication (SSL) is enabled between MySQL v5.0 and Chakra Max Manager v2.0 and between MySQL v5.0 and Chakra Max Server v2.0.

The additionally configured components in TOE operating environment are as follows.

[Table 1-2] Additional components

Component	Use
Mail Server	It sends the warning mail about the alert situation to a Security Administrator or provides the approval function to DB users though e-mail.
SMS Server	It sends a warning mail about alert situation to a Security Administrator.
Time Server	It provides reliable time-stamp to TOE and Protective DB.
Protective DB access tool	The application used for accessing the Protective DB.
Switch / TAP	Sniffing packet capture. Switch should be supported by Port Mirroring. TAP can be divided into UTP mode and the optic mode, and TAP used for operating TOE should be similarly configured in either mode.

1.4 TOE Description

It describes the physical/logical range of TOE in detail.

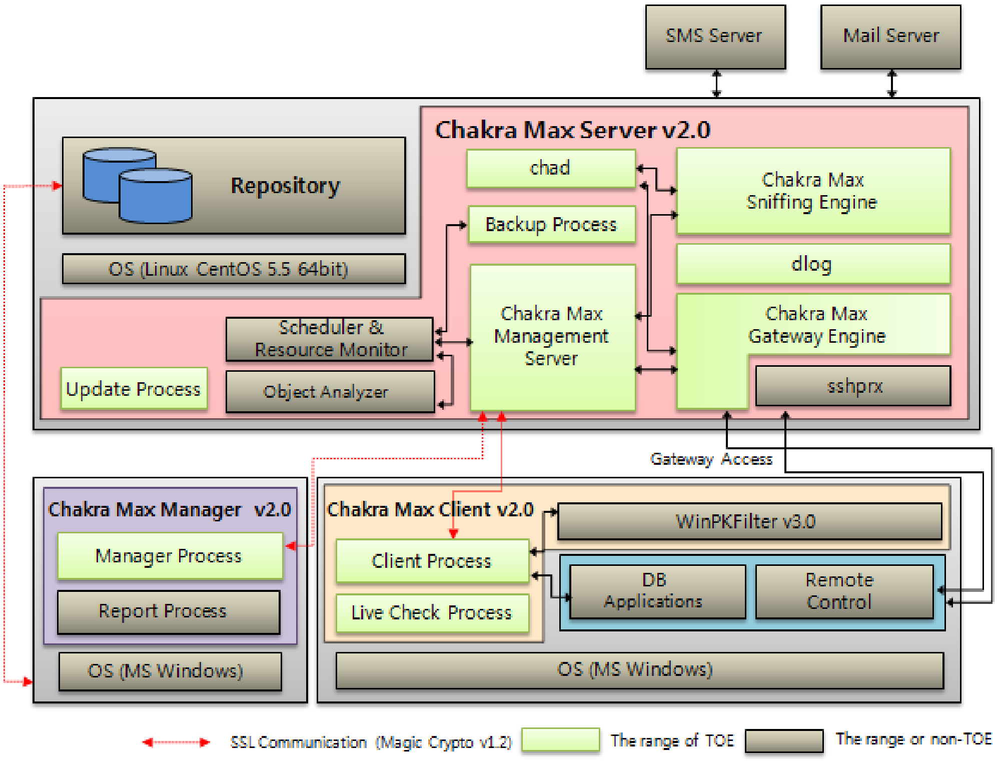
1.4.1 Physical range of TOE

The physical range of TOE is as follows:

[Table 1-3] TOE components

Component	Use
Chakra Max Server v2.0	It is part of TOE and a service of TOE that operates all the security functions.
Chakra Max Manager v2.0	It is part of TOE and a program which enables a Security Administrator to manage TOE security by GUI using CS mode.
Chakra Max Client v2.0	It is part of TOE and a program installed in Security Client User's PC which routes DB session and SQL automatically using a Gateway mode and provides GUI on which approval process can be used.
System administrator instructions	The documentation which describes the installation and operation methods of Chakra Max Server v2.0 to a Security Administrator.
Administrator instructions	The documentation which describes the installation and operation methods of Chakra Max Manager v2.0 to a Security Administrator.
User instructions	The documentation which describes the installation and operation methods of Chakra Max Client v2.0 to a Security Client User.

[[Figure 1-5] physical boundary] shows the physical boundary and range of TOE. The description of TOE within the range of evaluation is as follows.



[Figure 1-5] physical boundary of 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

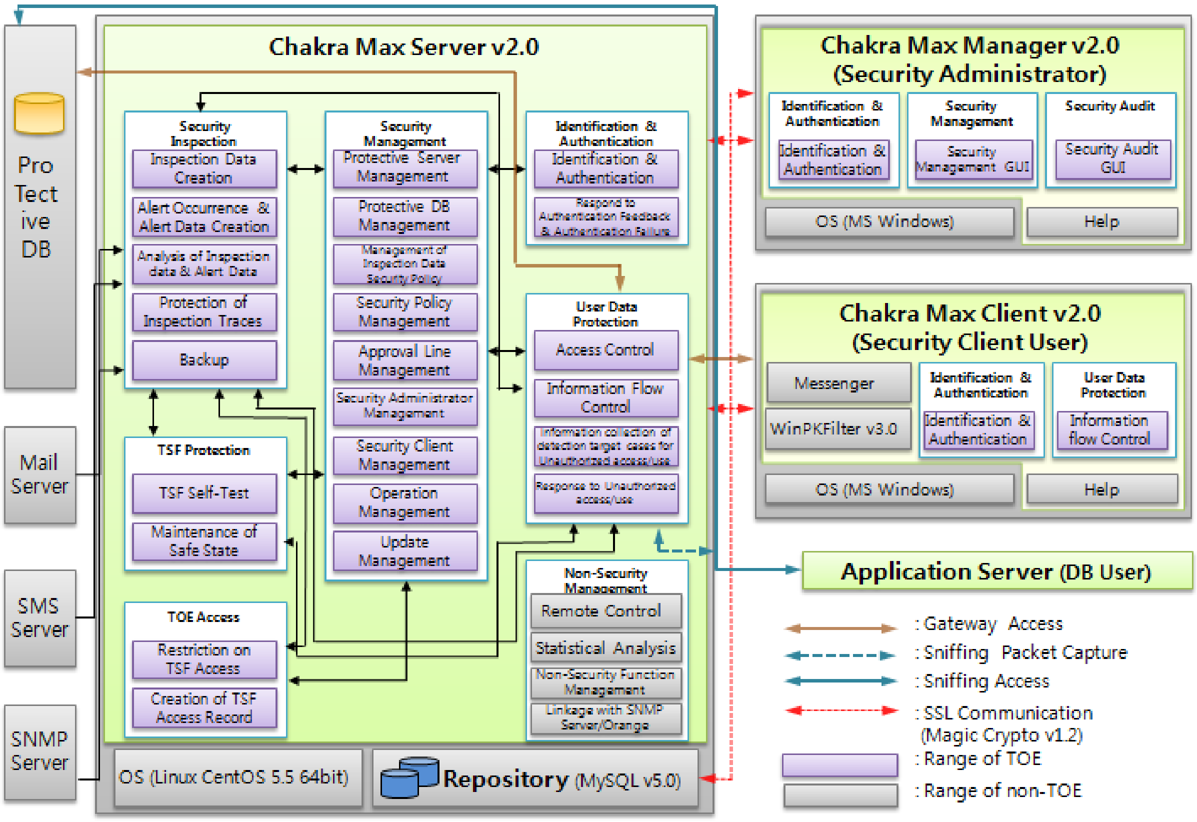
It executes Chakra Max Client v2.0 programs, communicates with Chakra Max Server v2.0 and plays a role in routing all data the Protective DB sends and receives via Chakra Max Server v2.0.

- 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.

1.4.2 Logical range of TOE

TOE provides such security functions as follows:


Pro
Tect
ive
DB
Mail Server
SMS Server
SNMP Server
Chakra Max Server v2.0
Security Inspection
Inspection Data Creation
Alert Occurrence & Alert Data Creation
Analysis of Inspection data & Alert Data
Protection of Inspection Traces
Backup
Security Management
Protective Server Management
Protective DB Management
Management of Inspection Data Security Policy
Security Policy Management
Approval Line Management
Security Administrator Management
Security Client Management
Operation Management
Update Management
Identification & Authentication
Identification & Authentication
Respond to Authentication Feedback & Authentication Failure
User Data Protection
Access Control
Information Flow Control
Information collection of detection target cases for Unauthorized access/use
Response to Unauthorized access/use
TSF Protection
TSF Self-Test
Maintenance of Safe State
TOE Access
Restriction on TSF Access
Creation of TSF Access Record
Non-Security Management
Remote Control
Statistical Analysis
Non-Security Function Managment
Linkage with SNMP Server/Orange
OS (Linux CentOS 5.5 64bit)
Repository (MySQL v5.0)
Chakra Max Manager v2.0
(Security Administrator)
Identification & Authentication
Identification & Authentication
Security Management
Security Management GUI
Security Audit
Security Audit GUI
OS (MS Windows)
Help
Chakra Max Client v2.0
(Security Client User)
Messenger
WinPKFilter v3.0
Identification & Authentication
Identification & Authentication
User Data Protection
Information flow Control
OS (MS Windows)
Help
Application Server (DB User)
: Gateway Access
: Sniffing Packet Capture
: Sniffing Access
: SSL Communication (Magic Crypto v1.2)
: Range of TOE
: Range of non-TOE

[Figure 1-6] Logical range of TOE

- Security audit

For all the packets collected by the packet filtering, TOE saves the audit data created in accordance with the Logging policy (default: all data are to be saved) as well as saving the Time-stamp to repository in chronological order.

The analysis of audit data and alarm data is implemented by the command from the Security Administrator; it consists of the real-time monitoring and the log search function.

Also, for the protection of the traces of audit and for the prevention of loss of audit data, the status will be notified to the Security Administrator by the alarm if the repository for the audit data is filled up to some level, i.e. 95%, and the security function is temporarily suspended until the capacity of repository is to be secured.

Backup function is provided in connection with the protection of audit traces. Backup is implemented on a regular basis by the scheduler or can be run manually by the user call. Backup stores the compressed audit data on a daily basis and deletes the original log which was saved in a backup to secure the space of repository according to configuration.

- User data protection

TOE provides the access control functions only to Security Client Users. It controls the access rights of Security Client User account and groups by DB to be protected.

There are two kinds of methods by which TOE controls information flow: Sniffing and Gateway.

First of all, in a Sniffing session of DB users, all the packets on the network are primarily collected and only the packets accessing the DB or the Server to be protected are collected by the filtering. For the collected information, the violations based on the security polity are inspected, and if some violations are found, the predefined actions against the unauthorized access or use are carried out.

In a Gateway session of the Security Client Users who gain access to the DB to be protected, the routing is made to Chakra Max Server v2.0 by Chakra Max Client v2.0; the violations are inspected on the basis of the security policy, and if there is no violation or if it is not subject to the approval of SQL, the function of information flow control is applied, which allows the packet exchange with the DB to be protected. If some security violation is found, TOE performs the predefined actions against the unauthorized access or use. The corresponding actions contain the function to create the alert data, the function to inform the Security Administrator (by sending e-mail or SMS) and the function of information flow control, which discards the specific packets, accompanied with the function to force the session to be terminated. Also, the SQL approval function is provided so that it can individually control the SQL implemented by the Security Client Users.

TOE provides the function of controlling the SQL initially generated in the Protective DB by way of New SQL Control policy in order to sort out security violations for the packets of **DB users.** Also, by inspecting Safe SQL and Work Time policy, it allows or controls information flow. And there is a function by which it provides DB users with the concealed important information of Protective DB table by applying the Masking policy.

- Identification and authentication

TOE provides the function of identification and authentication for Security Client Users and Security Administrators, based on IDs or/and passwords. When Security Administrators or Security Client Users fail to pass the authentication, the consecutive authentication attempts are prevented by locking up the account(s) that matter(s) for a few minutes according to TOE operating policy.

SSL function is utilized for the secured communication between Chakra Max Manager v2.0 and Chakra Max Server v2.0, between Chakra Max Client v2.0 and Chakra Max Server v2.0, between Chakra Max Server v2.0 and Repository, and between Chakra Max Manager v2.0 and Repository.

- Security administration

TOE is managed by Top-level Administrators having management privileges for all security functions and Normal Administrator granted management privileges for the selective security function by Top-level Administrators depending on security function access privileges.

In Security management, as Protective Server and Protective DB are added, there are function of modification, deletion and query, function of managing alert policy, masking policy and Approval policy, and function of saving only the particular audit data in Repository by setting Logging policy. Also, a function is provided for managing new SQL control policy which approves or control SQL explicitly according to the attribute of SQL, Safe SQL policy, and Work Time policy. And the approval limit management function is provided for approval function.

Also, as the accounts of TOE Security Administrator and Security Client User are added, a function of modification, deletion and query and the management function is also provided for controlling the access to Protective DB and Protective Server or deactivating the account.

In the administration of TOE operation, the function to administer the basic configuration data required for the performance of the TOE security function and the function to operate and terminate the TOE security engine are provided, and the administration function is provided to monitor the integrity of TSF data in real time.

Chakra Max Server v2.0 is manually updated by administrator. And when Chakra Max Manager v2.0 and Chakra Max Client v2.0 are in operation, auto update is made through TOE. Update file is located in the specific directory of Chakra Max Server v2.0 by an administrator, and TOE implements the integrity audit for the Update files and maintains the privacy protection by encrypted (SSL) communication to apply update to Chakra Max Manager v2.0 and Chakra Max Client v2.0

- TSF protection

When firstly loaded, after loaded, periodically, and when there is a request from a Security Administrator, TOE inspects the integrity of TSF data and TSF execution code integrity autonomously. When integrity error is found, it generates alert and notifies the Security Administrator by sending e-mail or SMS and suspends the security function to protect unreliable security audit.

When there is a disorder in MySQL v5.0, TOE saves audit data in the file system temporarily, and if MySQL v5.0 gets back to normal state, the temporarily saved audit data will be automatically saved in MySQL v5.0 so that the safe state can be maintained.

- TOE Access

TOE leaves the record of all the information (time, IP and activity) of Security Administrator who accessed TSF and this record provides the screen on which query is enabled in Work History. So, it enables Security Administrator to seek the details of TSF use.

Also when TOE authentication of Security Administrator happens, it shows the previous logon time so that the safety and security situation of a Security Administrator account can be checked. Also when Security Administrator and Security Client User do not use TOE for some time, the related session is to be locked up and reauthorization of secret number is requested so that the function of blocking the unauthorized TOE use is provided

1.4.3 The range of TOE

The functions which are not for assessment targets and not in the range of TOE are as follows:

- non-security management
  - Remote Control

Remote Control session (Telnet/SSH/FTP/R-CMD/Telnet) monitoring and controlling function is not in the range of TOE

- Statistical Analysis

Object Analyzer function which periodically or manually analyzes the record of acess to the main tables of the Protective DB, the monitoring function for system resource capacity and situation in Chakra Max Server v2.0, Object Usage analysis and Trend analysis function of SQL performance search results, and Statistical Analysis function such as Statistical Analysis for Protective DB, Protective Server and the security policy use and the statistical report function are not in the range of TOE.

- Non-security function management

The function of monitoring the overall situation and performance information by the Protective DB, schedule management function which registers and manages the performance cycle for statistics creation program that needs to be periodically performed by Chakra Max Core v2.0, and DB user holidays management function are not in the range of TOE.

- SNMP Server and Orange interworking

SNMP Server interworking function and the function of controlling the virtual Protective DB account added when Orange is interworked and the file approval function are not in the range of TOE.

- Other functions not provided by TOE
  - Messages sending and receiving function between Security Client Users
  - Help Function

- Hardware/Software/Firmware required in TOE

1.5 Rules for writing specification and definition of terms

This ST is written in Korean Hangul and for some abbreviated terms and for the clarified meaning, English is also used. The orthography, forms, and writing rules in use are in accordance with CC (CC v3.1r3). Also especially some words used in writing this ST are indicated.

1.5.1 Rules for writing specification

Each operation is used in this ST in the following form.

- Repeat

As the same component is repeated in various operations, it is used. The results of repeated operations are marked with the repeat number within the parenthesis after **component** identification letter, namely, '(repeat number)'.

- Allocation

It is used for allocating the specific values to parameters not specified in CC (for example, password length). The results of allocated operation are marked with the squared brackets, namely, [allocated_value].

- Selection

When the requirements are described, it is used for choosing one or more options provided in CC.

The results of selected operation are marked *in the underlined italic text*.

- Elaboration

It is used for restricting the requirements further by adding the details to CC. The results of Elaboration operation are marked in **bold text.**

- Caution in application

To clarify the meaning of requirements, to provide the information of options when it is realized and to define the criteria "appropriate/inappropriate" for the requirements, it is provided. Caution in application is provided with the relevant requirments if necessary.

1.5.2 Definition of terms

The terms used in this ST are in accordance with CC, and the following words are the terms additionally used in IT with some of other terms. The reason why they are described here is that it is intended to help the users who read this ST.

[Table 1-4] Definition of terms

Term	Description
Application Server	It is a middleware software server which access the Protective DB to perform stable transaction.
Chakra Max Server v2.0	It is a part of TOE and the service of TOE which performs all the security function
Chakra Max Client v2.0	It is a part of TOE and routes DB session and SQL automatically in a Gateway mode as installed in PCs of Security Client Users. It is a program that provides GUI on which approval process can be used
Chakra Max Manager v2.0	It is a part of TOE and a program that enables TOE security management through CS-mode GUI on which a Security Administrator can make TOE security management.
Passive	It means that the packets are only passively received without taking any action on the network.
Repository	Repository in which all the audit data of TOE are saved. It is composed of Linux CentOS 5.5 file system and MySQL v5.0.
Sensitive Object	Main table and Column information of the Protective DB
Single Mode	It indicates the TOE operating environment with a single Chakra Max Server v2.0 configured.

SSL (Secure Sockets Layer) V0.9.8k	Protocol developed by Netscape Co., Ltd. for exchanging the personal documents through the internet. SSL V0.9.8k is required because the internet protocol characteristically has some difficulty in maintaining the privacy in terms of security. In the e-commerce, it is widely used in the personal information or credit card security.
TAP (Test Access Point)	Passive mode device that can permanently make monitoring and analysis without affecting the data flow of the network at all.
TAR (Tape ARchive)	TAR (Tape ARchive) is a UNIX utility which zips the designated files into a file called as an archive or otherwise unzips it into the original files.
Ticker	An indicator that shows the alert issuing situation to a Security Administrator in real time.
TSF Data	Data for operating TOE performed to SFR directly and indirectly.
TSF execution code	Execution Code (Process) performed to SFR indirectly or directly for operating TOE.
Audit data	Information collective by TOE on performing access and query about the Protective DB.
Approval	Individual control mode for SQL performed by Security Client Users who gain unformatted access within TOE
Alert data	Information on the details of Alert situations due to TOE security policy.
Proposal	Requrest sent by a Drafter for approval to an Approver
Integrity	Blocking the unauthorized change in data and information and protecting them.
Security Administrator Role	A set of predefined rules which set the interaction to be allowed between a Security Administrator and TOE
Security policy	A set of rules that regulates the management, protection and distribution of assets within TOET
Protective DB	Database monitored and inspected by TOE..
Protective Server	Server in which Database monitored and inspected by TOE is installed..
Unformatted access	The pattern in which DB user or DBA access DB using DB access tools (Orange or SQL*Plus, etc.)
Switch	As a communication equipment which connects network units, it supports the packet transfer function to the specific computer.
Identity	The only expression which identifies the authorized user
Element	Inseparable minimum unit of security requirements
Operation	Activity which matches a component with the specific threat or meets the specific policy in CC (for example, repeat, allocation, selection, elaboration)

External IT Entity	All IT products or system, secured or unsecured, which interact with TOE externally (outside TOE)
Threat Agent	Unauthroized DB user, external IT entity or malicious internal administrator who bring threats such as unauthorized access, change or deletion, etc. to organizational assets.
Interface	It means the connection route or mode between the two independent systems. Also it implies the protocol used for access to hardware or software. For example, when personal computer and printer are accessed and if the two devices have the different standards, it is impossible to exchange the data. Only if they have the same standard, it is eventually possible to print out by the command of personal computer. At this time, we say that "the two devices are equipped with the same interface"
Formatted access	The pattern in which the Protective DB is accessed via application or middleware
Dependency Relation (Dependency)	Generally speaking, the relation between requirements that the dependent requirements must be satisfied to meet a target of a requirement.
Subject	Entity within TSC which generates the operation to be performed.

The users who are defined in this ST have the following names, roles and privileges.

[Table 1-5] Definition of roles

Name	Description
Administrator	TOE system operating manager for TOE installation, Update, or process audit, etc.
Security Administrator	It indicates all the authorized administrators who manage TSF using Chakra Max Manager v2.0. It includes Top-level Administrator and Normal Administrator. In this documentation what it means by "Security Administrator" denotes an administrator who is granted privilege about TSF specified in the relevant SFR.
Top-level administrator	It is an account registered at default after the installation of TOE. It is impossible to delete and add it. He has privileges to manage all TSF in TOE.
Normal administrator	He has privileges to manage TSF selectively granted by Top-level Administrator among the list of functions..
DB user	It indicates all the users who access the Protective DB. It includes all the Sniffing or Gateway access user.

<table>
<tr>
<td>Security Client User</td>
<td>DB users who access the Protective Server and Protective DB using Chakra Max Client v2.0. It implies Gateway access user, and regarding approval function Security Client Users have the following roles in detail.
<table>
<tr><th>Role</th><th>Description</th></tr>
<tr><td>Drafter</td><td>A Security Client User who has the privilege to access the Protective DB by drafting SQL to an Approver.</td></tr>
<tr><td>Approver</td><td>A Security Client User who has the privilege to approve the agenda requested by a Drafter.</td></tr>
<tr><td>DBA</td><td>A Security Client User who has the privilege to make a request to a Security Administrator by tuning SQL and approving the request of secured SQL from a Drafter in an interim process.</td></tr>
</table>
</td>
</tr>
</table>

2 Conformance claims

This ST conforms to the following evaluation criteria and in the conformance claims these are claimed.

2.1 CC Conformance

This ST conformance to the following CC.

- CC
  - CC for Information Technology Security Evaluation (Notification no. 2009-51 of Ministry of Public Administration and Security)
  - CC for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 Revision 3, 2009. 7, CCMB-2009-07-001
  - CC for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1 Revision 3, 2009. 7, CCMB-2009-07-002
  - CC for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1 Revision 3, 2009. 7, CCMB-2009-07-003

- Describes the conformance to CC as either:
  - This ST conformance to security requirements specified in Part 2 CC of information

protection system(Version 3.1 Revision 3) and the security the security assurance requirements specified in Part 3.

2.2 PP Conformance

There is no PP which this ST conformance to.

2.3 Package Conformance

This ST conforms to the following the security the security assurance requirements package.

- An assuarance package
  - Conformance to EAL4

3 Definition of Security problems

The definition of security problems specifies the security problems which should be dealt with in TOE and TOE operating environment and describes the assumptions about the related threat, organizational security policy (OSP) and TOE operating environment.

3.1 Threat

IT assets which TOE is designed to protect are the Protective DB operated by the organization, the data provided via the Protective DB and TOE itself. Threat agent has the advanced or basic level of professional knowledge, resources and motives and a threat agent who brings about the threat attacks TOE and protected rosources to make an attempt for the unauthorized access or steals important information in an unusual way for malicious use. He is an unauthorized DB user or external IT entity.

The threats to TOE are as follow.

[Table 3-1] Threats to TOE

Classification	Threats against TOE

T.Disguise	Threat agent may be an administrator in disguise to access TOE and change the security policy or compromise the security function.
T.Recording failure	When the capacity of saving in Repository is used up so that the security related events of TOE may not be recorded.
T.Failure to respond	TOE may not detect analyze or respond to a threat agent's unauthorized actions.
T.Unauthorized access to TOE	Threat agent may misuse TOE through the unauthorized access to TOE in a malicious way and bring about some unattempted actions.
T.A series of authentication ttempts	Threat agent may acquire the authorized administrator privileges by a series of attempts for authentication to access TOE and change the security policy or compromise the security function.
T.Unauthorized DB access	Threat agent may acquire the information of access to the Protective DB in an unusual way to make an attempt for the unauthorized access to DB and even if the access is permitted, he may access the data which he does not have the privielges about and query, change, delete the data.
T.TSF data damage	Threat agent may change or delete the saved TSF data in TOE in an unauthorized way to compromise the security function of TOE.
T.Detour	Threat agent may make a detour around the security function in TOE to access the Protective DB.
T.Transmitting data leakage	Threat agent may change or leak the data transferred by TSF through the network.

3.2 Organizational Security Policy (OSP)

TOE operating organizations have their own security policy and a Security Administrator realize the security policy by TOE which conforms to CC.

[Table 3-2] organizational security policy

Classification	Organizational security policy
P.Security audit	For seeking after the responsibility for the security-related actions, the security-related events should be recorded and maintained, and the saved data must be examined.

3.3 The assumptions about TOE operating environment

This ST assumes the following conditions in the security environment. of TOE.

[Table 3-3] Assumptions

Classification	Assumptions
A.physical security	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.Trusted administrator	A Security Administrator in 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.
A.The strengthening of Operating System	An administrator of TOE performs the task of removing all the uncessary 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.
A.Trusted repository	IT environment provides a reliable repository which saves the audit record. Repository may not be created, modified or deleted without the request of TOE.
A.Trusted external server	Mail Server and SMS Server for the email or SMS sending functions provided by TOE are located in the physically secured environment.
A.SSL authentication certificate of TOE	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.
A.SSL protocol	Since data communication channel between the separated TOEs are transferred while encrypted through SSL, the security from leaking out is guaranteed.
A.TIME	TOE is provided with reliable Time-stamp via a trusted administrator.
A.Unique connection point	In 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 TOE.
A.Trusted monitoring	TOE may monitor all the details about acess to the Protective DB.

4 Security Target

It describes the security targets of TOE security target, the security target and the theoretical ground about operating environment and proves that they correspond to the assumptions supported by threat, organizational security policy and security target.

4.1 Security targets of TOE

'Security target' describes the security targets for TOE and operating environment and suggests the theoretical ground that the described security targets support the security problems such as threat, organizational security policy or assumptions, etc.

[Table 4-1] TOE security target

Classification	TOE security target
O.Security audit	TOE should save and maintain the events to be able seek the responsibility for all the security-related activities such as the management of audit data, alert data and TSF data created while DB users have some interactions with the Protective DB and should provide the means by which the recorded audit data may be examined
O.Reliable audit	TOE should prevent the creation of unreliable data or the omission of audit data by responding autonomously to the emergency when there is an error in Repository or when space for saving is insufficient.
O.Security management	TOE should securely provide the means by which a Security Administrator of TOE may manage TOE effectively and should also provide the means by which TSF data can be kept most up to date.
O.TSF data protection	TOE should protect the important executable files for operating TOE and the TSF data saved in Repository from the unauthorized exposure, change, and deletion.
O.TSF data transfer protection	TOE should guarantee integrity and privacy of TSF data as it is transferred between the separated TOEs and between TOE and Repository.
O.Identification and uthentication	TOE should uniquely identify a Security Administrator and a Security Client User and authenticate the identity before allowing the access to TOE. Also, it should prevent the access by other IT environment than a Security Administrator to TOE and should provide some coping methods against

	authentication attempt attack/failure and reuse attack on authentication data
O.Detection of unauthorized access/use	TOE should analyze the collected data and detect whether or not there is an unauthorized access/use to the Protective DB.
O.Action against unauthorized access/use	TOE should take the appropriate action to protect the Protective DB according to the detection of the unauthorized access/use.

4.2 The security targets for operating environment

The security targets that are dealt with by IT areas or by non-technical/procedural means are as follow:

[Table 4-2] Security targets for TOE operating environment

Classification	Security targets for operating environment
OE.physical security	TOE should installed in the environment where the intranet is securely maintained by the network setting such as firewall. So, in other words, it should be located in the physically safe environment only a Security Administrator can access.
OE.trusted administrator	A Security Administrator in TOE is well trained about the TOE management function and should perform the management task in a correct and benign way according to the guidelines of, administrator.
OE.Strengthening operating system	An administrator of TOE should perform the task of removing all the uncessary services or methods in the operating system and strengthening the vulnerabilities in the operating system. He should guarantee the credibility and stability of the operating system of a server in which TOE is operated
OE.Trusted repository	IT environment should provide a trusted repository which saves the audit record. Repository should not be created, modified or deleted without the request of TOE.
OE.trusted external server	Mail Server and SMS Server for the email or SMS sending functions provided by TOE should be located in the physically secured environment.
OE.SSL authentication certificate of TOE	SSL authentication certificate of TOE should be securely created and managed

OE.SSL protocol	Data communication channel between the separated TOEs should be transferred while encrypted through SSL.
OE.TIME	Trusted administrator should take appropriate actions for providing the reliable time-stamp to TOE at all times by augumenting the operating system.
OE.unique connection point	In IT environment, if TOE is operated in a Gateway Mode and Hybrid Mode, the firewall should be installed at the front end of all the Protective DBs so that the environment should be provided in which every DB user may be forced to access the Protective DB only through TOE.
OE. Trusted monitoring	TOE should monitor all the details of access to the Protective DB.

4.3 Rationale of security targets

The rationale of security targes prove that the specified security target are suitable and sufficient for handling the security problems and that they are not excessive but necessary.

The rationale of security targets prove the following.

- Each assumption, threat, organizational security policy is handled by at least one security target.
- Each security target deals with at least one assumption, threat, or organizational security policy

[Table 4-3] Rationale of TOE security targets

Security targets Security environment	TOE security targets								Security targets for TOE operating environment									
	O.security audit	O.reliable audit	O.security management	O.TSF data protection	O.TSF data transferr otection	O.identification and authentication	O.unauthorized access/use detect	O.unauthorized access/use	OE.physical security	OE.trusted administrator	OE.operating system enhancement	OE.Reliable repository	OE.trusted external server	OE.TOE SSL authentication certificate	OE.SSL protocol	OE.TIME	OE.unique connection point	OE.trusted monitoring
T.disguise	✓					✓												
T. Recording failure		✓																

Security targets Security environment	TOE security targets								Security targets for TOE operating environment									
	O.security audit	O.reliable audit	O.security management	O.TSF data protection	O.TSF data transferr otection	O.identification and authentication	O.unauthorized access/use detect	O.unauthorized access/use	OE.physical security	OE.trusted administrator	OE.operating system enhancement	OE.Reliable repository	OE.trusted external server	OE.TOE SSL authentication certificate	OE.SSL protocol	OE.TIME	OE.unique connection point	OE.trusted monitoring
T. Failure to T.Respond	✓						✓	✓										
T.Unauthorized TOE access	✓		✓			✓												
T.A series of authentication attempt						✓												
T.Anauthorized DB access	✓						✓	✓										
T.TSF data damage	✓			✓														
T.Detour																	✓	
T.Leakage of transferred data					✓													
P.Security audit	✓																	
A.physical security									✓									
A.trusted administrator										✓								
A.Strengthening the operating system											✓							
A.Trusted repository												✓						
A.Trusted external server													✓					
A.SSL authentication Certificate of TOE														✓				

Security targets Security environment	TOE security targets								Security targets for TOE operating environment									
	O.security audit	O.reliable audit	O.security management	O.TSF data protection	O.TSF data transferr otection	O.identification and authentication	O.unauthorized access/use detect	O.unauthorized access/use	OE.physical security	OE.trusted administrator	OE.operating system enhancement	OE.Reliable repository	OE.trusted external server	OE.TOE SSL authentication certificate	OE.SSL protocol	OE.TIME	OE.unique connection point	OE.trusted monitoring
A.SSL protocol															✓			
A.TIME																✓		
A.Unique connection point																	✓	
A.Trusted monitoring																		✓

4.3.1 The theoretical ground of security targets for TOE

- **O. Security Audit**

  Since this security target guarantees that TOE should provide the means of saving and examining the security-related events, they correspond to threat T.disguise, T.unauthorized TOE access, T..TSF data damage, T.unauthorized DB access and T.failure to respond, and they are necessary for supporting organizational security policy and P.security audit.

- **O. Reliable audit**

  This security target is an autonomous coping method when there is an error in Repository or when space for saving is insufficient. Since it prevents the creation of unreliable audit data or the omission of audit data, it is necessary for coping with T. Recording failure.

- **O. Security management/administration**

  Since in this security target TOE provides a Security Administrator with the means of management by which he may securely access to TOE, it is necessary for coping with T.unauthorized TOE access.

- **O.TSF data protection**

  This security target is necessary for coping with T.TSF data damage since it should protect important executable files for operating TOE and TSF data saved within TOE from the unauthorized exposure or change.

- **O.TSF data transfer protection**

  This security target is necessary for coping with T. the leakage of transferred data since it should provide the means of protection and management of confidentiality and integrity of TSF data between the separated TOEs and between TOE and Repository.

- **O.identification and authentication**

  This security target is necessary for coping with T.disguise, T.unauthorized TOE access, and T.a series of authentication attempt threats since it prevents any other IT environment than a Security Administrator from accessing TOE, provides methods by which to take action against a series of authentication attempt attack/failure and authentication data reuse attack, and presents identification and authentication of a Security Administrator and DB users.

- **O.unauthorized access/use detection**

  This security target is necessary for responding to T.unauthorized DB access and T. Failure to respond since it provides the means by which to detect whether there is an unauthorized access/use to the protective.

- **O. Measures against unauthorized access/use**

  This security target is nessary for coping with T.unauthorized DB access, T. Failure to respond since according to the results of unauthorized access/use detection, it provides the means by which to protect the Protective DB.

4.3.2 Rationale of security targets for the operating environment

- **OE.physical security**

  This security target corresponds to A.physical security since only a Security Administrator can access TOE and it guarantees that TOE is located in the physically secured environment.

- **OE. Trusted administrator**

  This security target corresponds to A. trusted administrator since a Security Administrator of TOE is trusted and it guarantees that he can manage TOE securely..

- **OE. Strengthening the operating system**

  This security target corresponds to A. strengthening the operating system since it guarantees the operating system of TOE is secured and trusted by performing the tasks of removing all the services and means in the operating system not required by TOE and of strengthening the vulnerabilities in operating system.

- **OE. Reliable repository**

  This security target for the environment corresponds to the assumptions of A.Reliable repository since it provides a trusted Repository in which to save the audit data for the functions of TOE.

- **OE. Trusted external server**

  This security target for the environment corresponds to A.trusted external server since it guarantees that Mail Server and SMS Server provided by TOE which support the function for sending e-mail and SMS are located in the physically secured environment..

- **OE. SSL certificate of TOE**

  This security target for the environment corresponds to A. SSL authentication certificate of TOE since it guarantees that SSL authentication certificate of TOE is securely created and managed..

- **OE. SSL protocol**

  This security target for the environment corresponds to A.SSL protocol since it applies SSL protocol to the authentication of Security Administrator and DB user in TOE and to the data communication between the separated TOEs.

- **OE.TIME**

  This security target for the environment is necessary for supporting A.TIME since it is provided with the reliable time-stamp by a trusted administrator to keep trusted Time.

- **OE. unique connection point**

  This security target for the environment is necessary for supporting A.unique connection point and T.detour since it guarantees that in a Gateway Mode DB users can access the Protective DB only through TOE.

- **OE.Trusted monitoring**

  This security target for the environment corresponds to A.Trusted monitoring since it guarantees all the details of access to the Protective DB can be monitored..

5 Definition of expanded component

There is no expanded component this ST defines.

6 Security requirements

Security requirements describes the security functional requirements and the security the security assurance requirements provided in TOE which accepts CC.

6.1 The security functional requirements

The security functional requirements in this ST consist of security function components in CC (Version 3.1 Update edition 3) Part 2. The summary of security function components is shown as follows:

[Table 6-1] TOE the security functional requirements

Security function class	Security function components	
Security audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1(1)	Subset information flow control(1)
	FDP_IFC.1(2)	Subset information flow control(2)
	FDP_IFC.1(3)	Subset information flow control(3)
	FDP_IFC.1(4)	Subset information flow control(4)
	FDP_IFC.1(5)	Subset information flow control(5)
	FDP_IFF.1(1)	Simple security attributes(1)
	FDP_IFF.1(2)	Simple security attributes(2)
	FDP_IFF.1(3)	Simple security attributes(3)
	FDP_IFF.1(4)	Simple security attributes(4)
	FDP_IFF.1(5)	Simple security attributes(5)

Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	TSF data management
	FMT_MTD.2	Management of limits on TSF data
	FMT_SAE.1(1)	Time-limited authorization(1)
	FMT_SAE.1(2)	Time-limited authorisation(2)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on security roles
	FMT_SMR.3	Assuming roles
TSF protection	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps
	FPT_TRC.1	Internal TSF consistency
	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.1	TSF-initiated session locking

[Table 6-2] List of subject and object shows 'subject and object' defined by this the security functional requirements according to the operation

[Table 6-2] List of subject and object

Subject	Object	Attribute	Operation
Top-level Administrator	Normal Administrator account	Normal Administrator identity, security function performing privileges, account validity term, alert receiving information	creation, query, modification, deletion
Top-level Administrator, Normal Administrator	DB user session	DB user's identity, Protective DB access information, access date, SQL information	query, deletion
	security policy	applicable DB user's identity, validity term, policy target SQL information, Protective DB information, approval-related information	creation, query, modification,

			deletion
	Approval line	Approver's identity, approval level, proxy approval, urgent approval information	creation, query, modification, deletion
	audit data save policy	DB user's identity, Protective DB information, SQL, date	creation, query, modification, deletion
	audit data	DB user's identity, Protective DB information, SQL, date, policy change information, environment variable change information, identification and authentication information	query
	alarm data	DB user's identity, SQL information, security policy information, alert-emitting related information, Protective DB information	query
	Protective DB, Protective Server information	Protective Server information, Protective DB information	creation, query, modification, deletion
	TOE environment setting data	environment configuration information required for operating TOE	creation, query, modification, deletion
	integrity audit	integrity audit items	start
	Backup	Backup information, recovery information	start
	Security Client User account	Security Client User identity, validity term	creation, query, modification, deletion
Security Client User	Security Client User account	secret number, telephone number, E-Mail address	modification
	SQL approval information	Protective DB information, approval-related information, validity term, SQL execution restriction count, SQL sentence	creation, query, modification, deletion
Security Client	Protective DB	SQL sentence	creation,

User, DB user			query, modification, deletion

6.1.1 Security audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [floating security violation alarm message selectively, sending the warning mail to a Security Administrator, or sending text message (SMS), etc.] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamp

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [Not Available]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [date, time, Security Administrator information, **DB user** information, and audit target event information].

[Table 6-3] Audit target event

Function components	Audit target events
FAU_ARP.1	Actions taken due to potential security violations.
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms.
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.
FDP_IFF.1(1)	Decisions to permit requested information flows.
FDP_IFF.1(2)	Decisions to permit requested information flows.
FDP_IFF.1(3)	Decisions to permit requested information flows.
FDP_IFF.1(4)	Decisions to permit requested information flows.
FDP_IFF.1(5)	Decisions to permit requested information flows.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions.
FIA_UAU.2	Unsuccessful use of the authentication mechanism. All use of the authentication mechanism.
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided
FMT_SMF.1	Use of the management functions.
FMT_SMR.2	Modifications to the group of users that are part of a role. Unsuccessful attempts to use a role due to the given conditions on the roles.
FMT_SMR.3	Explicit request to assume a role.
FPT_STM.1	Changes to the time.
FPT_TRC.1	Restoring consistency upon reconnection.
FAU_STG.3	Actions taken due to exceeding of a threshold.
FAU_STG.4	Actions taken due to the audit storage failure.

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Caution in application: a user's identity means Chakra Max Client v2.0 account information and information of DB user's access session, which can identify the user.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [audit data] known to indicate a potential security violation;

b) [Not Available].

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data creation

FAU_SAR.1.1 The TSF shall provide [Security Administrator] with the capability to read [all audit data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the **Security Administrator** to interpret the information.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [audit data filtering and sequencing] of audit data based on [the standard with the following logical relations].

a) logical relation targets

- subject identity
- subject direction
- object identity
- object reponse
- event date and time
- event type
- event importance(level)
- event control information
- security policy information
- keyword

b) In the logical relation targets above, the logical relation between the items is AND, and OR is applied within an item.

Caution in application: Among audit data, what are to be saved in the File system, such asstartup, shutdown and update, etc. of TOE, do not support the search by filtering and sequencing.

FAU_SEL.1 Selective audit

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) *subject identity, object identity, event type*

b) [audit event selectable targets

- subject command
- object response
- event date and time]

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [issuing an alert or informing a Security Administrator by e-mail or SMS ,etc.] if the audit trail exceeds [90 % of the total allocated disk space].

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [ignore audited events] and [issuing the alert, or informing a Security Administrator by e-mail or SMS, etc.] if the audit trail is full.

6.1.2 User data protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [access control policy] on [Security Client User's access to the Protective DB].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [access control policy] to objects based on the following: [security attributes about the following subjects and objects].

a) subject attributes

- Security Client User Group name
- Security Client User account
- Security Client User IP address

b) object attributes

- Protective DB Group name
- Protective DB Name

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [access privilege allocation].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [Not Available].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [Not Available].

FDP_IFC.1(1) Subset information flow control(1)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(1) Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Alert policy] on [the operation used by the following subjects for the object].

a) Subject

- Security Client User
- DB User

b) Object

- Protective DB

c) Operation

- Security Client User session information and SQL
- DB user session information and SQL

d) List of Alert policy

- outbreak alert, Kill Session, Reject SQL

FDP_IFC.1(2) Subset information flow control(2)

Hierarchical to: No other components.
Dependencies: FDP_IFF.1(2) Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Masking policy] on [information brought by the following subject from the object].

a) subject

- Security Client User

b) object

- Protective DB

c) Masking policy list

- Full Masking, Partial Masking

FDP_IFC.1(3) Subset information flow control(3)

Hierarchical to: No other components.
Dependencies: FDP_IFF.1(3) Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Approval policy] on [the operation used by the following subjects for the object].

a) subject

- Security Client User

b) object

- Protective DB

c) operation

- Security Client User session information and SQL

- DB user session information and SQL

b) Approval policy list

- approval approval request

FDP_IFC.1(4) Subset information flow control(4)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(4) Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [New SQL Control policy] on [the operation used by the following subjects for the object].

a) subject

- DB user

b) object

- Protective DB

c) operation

- SQL

d) New SQL policy list

- Alert Only, Kill Session

FDP_IFC.1(5) Subset information flow control(5)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(5) Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Safe SQL policy] on [the operation used by the following subjects for the object].

a) subject

- Security Client User

b) object

- Protective DB

c) operation

- SQL

d) Safe SQL policy list

- approval approval request

FDP_IFF.1(1) Simple security attributes(1)

Hierarchical to: No other components.
Dependencies: FDP_IFC.1(1) Subset information flow control(1)
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [Alert policy] based on the following types of subject and information security attributes: [the following].

a) subject security attributes

- IP address, Computer name, OS User name, Application name, MAC address
- Security Client User name, Security Client User group name

b) information security attributes

- Date of access, SQL sentence(Type, Text, Command) information, query size, time while session is not used, SQL number
- SQL resultvalue, SQL responsetime, SQL result line number, response query size, SQL result code

c) object security attribute

- Protective DB Name, access accountinformation, Table information, Column information

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Not Available].

FDP_IFF.1.3 The TSF shall enforce the [selection of subject and object to which security policy is applied].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [Safe SQL policy].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [New SQL Control policy].

FDP_IFF.1(2) Simple security attributes(2)

Hierarchical to: No other components.
Dependencies: FDP_IFC.1(2) Subset information flow control(2)

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [Masking policy] based on the following types of subject and information security attributes: [the following].

a) subject security attributes

- IP address, computer name, OS User name, Application name, MAC address
- Security Client User name, Security Client User Group name

b) information security attributes

- access date, SQL sentence (Table, Column) information

c) object security attributes

- Protective DB Name, access accountinformation, Table information, Column information

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Not Available].

FDP_IFF.1.3 The TSF shall enforce the [selection of subject and object to which a security policy will be applied].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [Not Available].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [Alert policy and Approval policy].

FDP_IFF.1(3) Simple security attributes(3)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(3) Subset information flow control(3)
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [Approval policy] based on the following types of subject and information security attributes: [the following].

a) subject security attributes

- IP address, computer name, OS User name, Application name, MAC address
- Security Client User name, Security Client User Group name

b) information security attributes

- access date, SQL sentence (Type, Text, Command) information
- approval line, in-use period, usage count

c) object security attributes

- Protective DB Name, access accountinformation, Table information, Column information

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [SQL post-approval].

FDP_IFF.1.3 The TSF shall enforce the [selection of subject and object to which a security policy will be applied].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [Safe SQL policy].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [Alert policy (Reject SQL and Kill Session)].

FDP_IFF.1(4) Simple security attributes(4)

Hierarchical to: No other components.
Dependencies: FDP_IFC.1(4) Subset information flow control(3)
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [New SQL Control policy] based on the following types of subject and information security attributes: [the following].

a) subject security attribute : Not Available

b) information security attribute

- SQL, period

c) object security attribute

- Protective DB Name

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Not Available].

FDP_IFF.1.3 The TSF shall enforce the [selection of object to which a security policy will be applied].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [Not Available].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [Alert policy].

FDP_IFF.1(5) Simple security attributes(5)

Hierarchical to: No other components.
Dependencies: FDP_IFC.1(5) Subset information flow control(5)
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [Safe SQL policy] based on the following types of subject and information security attributes: [the following].

a) subject security attribute : Not Available
b) information security attribute

- SQL, duration

c) object security attribute

- Protective DB Name

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Not Available].

FDP_IFF.1.3 The TSF shall enforce the [Not Available].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [Not Available].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [Not Available].

6.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***Security Administrator*** *can set [from 3 to 10]**(default: 3),*** unsuccessful authentication attempts occur related to [a Security Administrator's TOE authentication failure or a Security Client User's TOE authentication failure].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall [the delaying of authentication for a time which a Security Administrator can set/configure from 1 to 43200(minutes)(default: 10 min)].

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[identifier, secret number, the state setting value(normal, suspension, delay), authentication failure count, privileges(Security Administrator, Security Client User)]

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the acceptable standards as follows].

a) password length should be from 8 letters or more to 16 letters or less, and the password should be made by a combination of alphabet, numeric, and special character.

b) the possible characters are as follows:

- alphabet a-z, A~Z : a capital[small] letter classification, 52 letters

- numeric 0-9 : 10 letters
- special character `~!@#$%^&*()-_=+[]{}₩|;:‘’“”,.<>/? : 32 letters

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **Security Administrator and Security Client User** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [‘*’ for secret number entry] to the **Security Administrators and Security Client Users** while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **Security Administrators and Security Client Users** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *decide, suspend, launch and change the action of* the functions [following] to [Security Administrator] .

a) List of functions

- Setting up the TOE operating environment
- Protective Server, Protective DB management
- Protective DB access session and SQL monitoring and real-time control
- Security Client User Protective DB access privileges control
- Security client user Protective DB access session and SQL control through alert policy
- Hiding the main table data information of the Protective DB through Masking policy
- SQL control through Approval policy
- Setting up new SQL control policy
- Granting the work flexibility through setting the Safe SQL policy
- Pre-setup of approval
- Saving the audit data selectively through Logging policy
- general work time control of Security Client User
- Security Administrator account management (applicable only to Top-level Administrator among Security Administrators)
- Security Client User account management
- Perfoming TSF data integrity Test at the request of Security Administrator
- audit data and alert data query
- audit data Backup setup
- TOE Update management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [the following security policies] to restrict the ability to *query, modify* the security attributes [the following] to [Security Administrator and Security Client User].

[Table 6-4] Security policy by security attribute

Security policies	Security attributes
access controlpolicy (Security Administrator inquiry/change)	a) subject attribute ■ Security Client User Group name ■ Security Client User account ■ Security Client User IP address ■ Security Client User working time b) object attribute ■ Protective DB Group name ■ Protective DB Name
Alert policy (a Security Administrator's inquiry/change)	a) subject security attribute ■ IP address, computer name, OS User name, Application name, MAC address ■ Security Client User name, Security Client User Group name b) information security attribute ■ access date, SQL sentence(Type, Text, Command) information, query size, time while session is not used, SQL number ■ SQL resultvalue, SQL responsetime, SQL result line number, response query size, SQL result code c) object security attribute ■ Protective DB Name, access accountinformation, Table information, Column information
Masking policy (a Security Administrator's inquiry/change)	a) subject security attribute ■ IP address, computer name, OS User name, Application name, MAC address ■ Security Client User name, Security Client User Group name b) information security attribute ■ access date, SQL sentence(Table, Column) information c) object security attribute ■ Protective DB Name, access accountinformation, Table information, Column information, Policy Item Group
Approval policy (a Security Administrator's inquiry/change)	a) subject security attribute ■ IP address, computer name, OS User name, Application name, MAC address ■ Security Client User name, Security Client User Group name b) information security attribute ■ access date, SQL sentence(Type, Text, Command) information

	■ approval line, in-use period, usage count c) object security attribute ■ Protective DB Name, access account information, Table information, Column information
New SQL Control policy (a Security Administrator's inquiry/change)	a) information security attribute ■ SQL, period b) object security attribute ■ Protective DB Name
Safe SQL policy (a Security Administrator's inquiry/change)	a) information security attribute ■ SQL, period b) object security attribute ■ Protective DB Name
Logging policy (a Security Administrator's inquiry/change)	a) subject security attribute ■ IP address, computer name, OS User name, Application name, MAC address b) information security attribute ■ access date, SQL sentence(Type, Text, Command) information c) object security attribute ■ Protective DB Name, access account information, Table information, Column information, Policy Item Group
Work Time setting (a Security Administrator's inquiry/change)	a) information security attribute ■ access day and time b) object security attribute ■ Protective DB Name
server and DB registration (a Security Administrator's inquiry/change)	a) subject security attribute ■ Security Client User name, Security Client User Group name b) object security attribute ■ Protective Server name, Protective DB Name
Backup management (a Security Administrator's inquiry/change)	a) information security attribute ■ Backup time, Backup location/file name, audit data target for automatic deletion b) object security attribute ■ E-Mail notification information
Security Client User management	a) object security attribute ■ Security Client User account, Security Client User name, secret

(a Security Administrator's inquiry/change)	number, validity term, telephone number, E-Mail address, description, IP address, Security Client User Group name
Security Client User management (a Security Client User's inquiry/change)	a) object security attribute ■ secret number, telephone number, E-Mail address, Approver on one's behalf, period of approval on one's behalf
Security Administrator management (a Top-level Administrator's inquiry/change)	a) object security attribute ■ Security Administrator account, Security Administrator 명, secret number, validity term, telephone number, mobile phone number, E-Mail address, description, IP address, Security Administrator privilege name, Alert Call Level, SMS or E-Mail receiving situation, Protective DB Name, Protective Server name
Security Administrator management (a Security Administrator's inquiry/change)	a) object security attribute ■ secret number, telephone number, mobile phone number, E-Mail address, Alert Call Level, SMS or E-Mail received or not received
User Profile setup (a Security Administrator's inquiry/change)	a) object security attribute ■ Security Administrator and Security Client User secret number change cycle, secret number authentication failure count and account lockup time
Environment setup (a Security Administrator's inquiry/change)	a) object security attribute ■ whether or not use language setting, Alert information File is saved, whether or not Predefined Security Alert monitoring is in use, SQL execution log saving location, whether or not the changed security policy is applied to session in use, whether or not SQL Parser is applied, whether or not Remarks is included in a sentence when saving SQL, policy violation IP session block time, SMTP-related information, SMS-related information, whether or not the client IP is controlled, whether or not the same account is allowed at the multiple login, multiple login number setup, online update-related information, SNMP-related information, whether or not Orange is used, Debug Log Level setup, NIC device-related information, Schedule job-relatedinformation, temporary saving directory setup when there is an error in Repository

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [function of TOE for setting the environment] to provide *[recommended]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Security Administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *modify, [activate or inactivate]* the [following *TSF* data list] to [the following Security Administrators].

a) Top-level Administrator

- ■ all the specified security attributes in [Table 6-4]

b) Normal Administrator

- ■ all the security attributes specified in [Table 6-4] (Top-level Administrator's security attributes excluded)

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [all the security attributes stipulated in [Table 6-4]] to [Security Administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [requesting the resetting after printing out the error message].

FMT_SAE.1(1) Time-limited authorization(1)

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [secret number of Security Administrators and Security Client Users] to [Security Administrator].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [the message window indicating the change of secret number is needed] **from 7 days before** for the indicated security attribute has passed.

FMT_SAE.1(2) Time-limited authorization(2)

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [the expiration time of validity term of TOE Access by Security Administrators and Security Client Users] to [Security Administrator].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [blocking a Security Administrator's and a Security Client User's TOE Access] after the expiration time for the indicated security attribute has passed.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[a) security function management : the item specified in FMT_MOF.1.

b) security attribute management : the item specified in FMT_MSA.1.

c) TSF data management : the item specified in FMT_MTD.1, FMT_MTD.2.

d) security role management : the item specified in FMT_SMR.2, FMT_SMR.3.

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: [the following Security Administrators and Security Client Users].

[Table 6-5] TOE administrator identification

classification	roles and privileges
Security Administrator	It denotes all the authorized administrators who manage TSF using Chakra Max Manager v2.0. It includes Top-level Administrators and Normal Administrators, and what it means by "Security Administrator" in this document indicates an administrator granted privileges for TSF specified in the relevant SFR.
Top-level Administrator	An account registered at default after the installation of TOE. It is impossible to delete or add it. It has the privilege to manage all TSF of TOE.
Normal Administrator	It has the management privilege for TSF which is selectively granted by a Top-level Administrator in the list of functions.

[Table 6-6] TOE user identification

<table>
<tr><th>classification</th><th colspan="2">roles and privileges</th></tr>
<tr><td rowspan="5">Security Client User</td><td colspan="2">It denotes DB users who access to the Protective DB using Chakra Max Client v2.0. It means users who access in a Gateway Mode. With regard to the approval function, a Security Client User has the following roles in detail.</td></tr>
<tr><td>role</td><td>description</td></tr>
<tr><td>Drafter</td><td>A Security Client User who is granted the privilege to access the Protective DB by drafting SQL to an Approver.</td></tr>
<tr><td>Approver</td><td>A security client user having an approval privilege for the agenda requested by a Drafter.</td></tr>
<tr><td>DBA</td><td>A Security Client User having a privilege to make</td></tr>
</table>

		a request to a Security Administrator by tuning SQL and approving Safe SQL request from a Drafter at the interim stage.

FMT_SMR.2.2 The TSF shall be able to associate **Security Administrators and Security Client Users** with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [conditions for the roles according to Security Administrator's TSF management privileges] are satisfied.

a) Security Administrator TSF management privileges selective item

[Table 6-7] Security Administrator TSF management privileges selective item

Selective item of Management privileges by TSF	Description
Monitor	the privilege to inspect the Protective DB access session information and Alert status and SQL perfoming situation and information in real time
Policy	the privilege to manage logging policy, alert policy, Masking policy, Approval policy, New SQL policy, Safe SQL policy, approval line setup, a Security Client User's Work Time control setting value, and a Security Administrator's and a Security Client User's identification and authentication setting value
Search	the privilege to query the audit data about the Protective DB, approval, security client, and Security Administrator and Alert alert data
System	the privilege to manage the Protective Server, the Protective DB, Security Client Users and the privilege for the audit data Backup, TOE operating environment setup, TSF data integrity audit

b) Security Administrator TSF management privileges attribute

- View
- Modify

FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [a Approver].

6.1.5 TSF protection

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [an error in the main process and Repository required for operating, insufficient space for saving the audit data in Repository].

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 **An administrator** shall be able to provide reliable time stamp **through the operating system.**

FPT_TRC.1 Internal TSF consistency

Hierarchical to: No other components.
Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [the update of Chakra Max Manager v2.0 and Chakra Max Client v2.0].

FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, [at the request of Security Administrator]* to demonstrate the correct operation of *TSF*.

FPT_TST.1.2 The TSF shall provide authorised **Security Administrators** with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorised **Security Administrators** with the capability to verify the integrity of *TSF*.

6.1.6 TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after [a time(minute) of not-in-use period from 1 to 1440 minutes(default: 3) a Security Administrator can configure for which TOE is not used by Security Administrators or Security Client Users] by:

a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [the reauthentication of secret numbers of Security Client Users or Security Administrators].

6.2 The security the security assurance requirements

The security the security assurance requirements in this ST consists of assuarance component of CC (v3.1r3) Part 3, and assessment assuarance level is EAL4. The following is a summary of assuarance components.

[Table 6-8] TOE the security the security assurance requirements

Assuarance class	Assuarance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of Security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

6.2.1 Development

ADV_ARC.1 Security architecture description

Dependencies ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4 Complete functional specification

Dependencies ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_IMP.1 Implementation representation of the TSF

Dependencies ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3 Basic modular design

Dependencies ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.2 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 Life-cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.4 Problem tracking CM coverage

Dependencies No dependencies.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 Identification of security measures

Dependencies No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce and provide development security documentation.

Content and presentation elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4 Security Target evaluation

ASE_INT.1 ST introduction

Dependencies No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies ASE_OBJ.2 Security objectives
ASE_ECD.1 Expanded component definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Basic design test

Dependencies ADV_ARC.1 Security architecture description
ADV_TDS.2 Architectural design
ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Function test

Dependencies ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

AVA_VAN.3 Focused vulnerability analysis

Dependencies ADV_ARC.1 Security architecture description
ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_DPT.1 Testing: basic design

Developer action elements:

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6.3 The theoretical ground of security requirements

The theoretical ground of security requirements proves that the described IT security requirements are suitable for satisfying the security target and are appropriate to handle security problems as a result.

6.3.1 The theoretical ground of the security functional requirements

The theoretical ground of TOE the security functional requirements proves the following things.

Each TOE security target is handled at least by more than a TOE security functional requirements, and each TOE security functional requirements handles at least more than a TOE security target.

[Table 6-9] The relation between the security functional requirements and security targets

security target / the security functional requirements	O.Security audit	O.Reliableaudit	O.Security management	O.TSF data protection	O.TSFdata 전송protection	O.Identification and authentication	O.Unauthorized access/use detect	O.Coping with unauthorized access/use	O.TIME
FAU.ARP.1								✓	
FAU.GEN.1	✓								
FAU.GEN.2	✓					✓			
FAU_SAA.1	✓						✓		
FAU_SAR.1	✓						✓		
FAU_SAR.3	✓								
FAU_SEL.1	✓								
FAU_STG.1				✓					
FAU_STG.3		✓		✓					
FAU_STG.4		✓		✓					
FDP_ACC.1							✓	✓	
FDP_ACF.1							✓	✓	
FDP_IFC.1(1)							✓	✓	
FDP_IFC.1(2)							✓	✓	
FDP_IFC.1(3)							✓	✓	
FDP_IFC.1(4)							✓	✓	
FDP_IFC.1(5)							✓	✓	
FDP_IFF.1(1)							✓	✓	
FDP_IFF.1(2)							✓	✓	

security target / the security functional requirements	O.Security audit	O.Reliableaudit	O.Security management	O.TSF data protection	O.TSFdata 전송protection	O.Identification and authentication	O.Unauthorized access/use detect	O.Coping with unauthorized access/use	O.TIME
FDP_IFF.1(3)							✓	✓	
FDP_IFF.1(4)							✓	✓	
FDP_IFF.1(5)							✓	✓	
FIA_AFL.1						✓			
FIA_ATD.1						✓			
FIA_SOS.1						✓			
FIA_UAU.2						✓			
FIA_UAU.7						✓			
FIA_UID.2						✓			
FMT_MOF.1			✓						
FMT_MSA.1			✓						
FMT_MSA.3			✓						
FMT_MTD.1			✓						
FMT_MTD.2			✓						
FMT_SAE.1(1)			✓						
FMT_SAE.1(2)			✓						
FMT_SMF.1			✓						
FMT_SMR.2			✓						
FMT_SMR.3			✓						
FPT_FLS.1				✓					
FPT_ITT.1					✓				

security target / the security functional requirements	O.Security audit	O.Reliableaudit	O.Security management	O.TSF data protection	O.TSFdata 전송protection	O.Identification and authentication	O.Unauthorized access/use detect	O.Coping with unauthorized access/use	O.TIME
FPT_STM.1									✓
FPT_TRC.1					✓				
FPT_TST.1				✓					
FTA_SSL.1				✓		✓			

Each security functional requirements satisfies the TOE security target as follows:

- FAU.ARP.1

  This SFR corresponds to O.Response to unauthorized access/use since it informs an administrator using a warning message, mail and SMS as soon as detecting unauthorized access/use

- FAU.GEN.1

  This SFR corresponds to O.Security audit since it creates the audit record of audit target events.

- FAU.GEN.2

  This SFR corresponds to O.Security audit and O.Identification and authentication since it can link users who generate the event with regard to the audit event.

- FAU_SAA.1

  This SFR corresponds to O.Security audit and O.Unauthorized access/use detection since it provides the analysis of the inspected event.

- FAU_SAR.1

  This SFR corresponds to O.Security audit and O.Unauthorized access/use detection since it provides a Security Administrator with the function for examining the audit data.

- FAU_SAR.3

  This SFR corresponds to O.Security audit since it provides the audit data filtering and ordering, etc.

- FAU_SEL.1

  This SFR corresponds to O.Security audit since it provides the capacity to select a set of audit target events from the audit data.

- FAU_STG.1

  This SFR corresponds to O.TSF data protection since it provides the function for protecting the audit trace repository.

- FAU_STG.3

  This SFR corresponds to O.Reliable audit, O.TSF data protection since it provides the expection of audit data loss and the coping action.

- FAU_STG.4

  This SFR corresponds to O.Reliable audit and O.TSF data protection since it provides the coping action by which the audit data loss can be prevented.

- FDP_ACC.1

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the function of partial access control for the Protective DB.

- FDP_ACF.1

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the security attributes for the access control function.

- FDP_IFC.1(1)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use protective since it provides the function of partial information flow control for the DB.

- FDP_IFC.1(2)

This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the function of partial information flow control for the Protective DB.

- FDP_IFC.1(3)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the function of partial information flow control for the Protective DB.

- FDP_IFC.1(4)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the function of partial information flow control for the Protective DB and the function of collecting the information for the basis of information flow control.

- FDP_IFC.1(5)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the function of partial information flow control for the Protective DB and the function of collecting the information for the basis of information flow control.

- FDP_IFF.1(1)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the security attributes for the function of information flow control.

- FDP_IFF.1(2)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the security attributes for the function of information flow control.

- FDP_IFF.1(3)

  This SFR information flow provide security attribute on control function, corresponding to O.Unauthorized access/use detection, O.Response to unauthorized access/use.

- FDP_IFF.1(4)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the security attributes for the function of information flow control.

- FDP_IFF.1(5)

  This SFR corresponds to O.Unauthorized access/use detection and O.Response to unauthorized access/use since it provides the security attributes for the function of information flow control.

- FIA_AFL.1

  This SFR corresponds to O.Identification and authentication since it provides the function of detection of and response to the authentication failure of a Security Administrator and a Security Client User.

- FIA_ATD.1

  This SFR corresponds to O.Identification and authentication since it provides the attributes for a Security Administrator and a Security Client User.

- FIA_SOS.1

  This SFR describes combination rule of secret number for Security Administrator and Security Client User account, corresponding to O.Identification and authentication.

- FIA_UAU.2

  This SFR corresponds to O.Identification and authentication since it provides the authentication of a Security Administrator and a Security Client User.

- FIA_UAU.7

  This SFR corresponds to O.Identification and authentication since it provides the protection of authentication feedback of a Security Administrator and a Security Client User.

- FIA_UID.2

  This SFR corresponds to O.Identification and authentication since it provides the identification of a Security Administrator and a Security Client User with regard to TSF use.

- FMT_MOF.1

  This SFR corresponds to O.Security management since it provides the management of all the functions of TOE.

- FMT_MSA.1

  This SFR corresponds to O.Security management since it provides the security attributes for the TOE function.

- FMT_MSA.3

  This SFR corresponds to O.Security management since it provides the default value with regard to TOE security attribute.

- FMT_MTD.1

  This SFR corresponds to O.Security management since it provides the management of TSF data.

- FMT_MTD.2

  This SFR corresponds to O.Security management since it specifies the function of the limit value management for TSF data.

- FMT_SAE.1(1)

  This SFR corresponds to O.Security management since it provides the management of the validity term of secret numbers of a Security Administrator and a Security Client User.

- FMT_SAE.1(2)

  This SFR corresponds to O.Security management since it provides the management of validity term of TOE access for a Security Administrator and a Security Client User.

- FMT_SMF.1

  This SFR corresponds to O.Security management since it specifies the management function of TSF.

- FMT_SMR.2

  This SFR corresponds to O.Security management since it specifies the restriction of security roles for each Security Administrator.

- FMT_SMR.3

  This SFR corresponds to O.Security management since it provides the role delegation for some functions.

- FPT_FLS.1
  This SFR corresponds to O.TSF data protection since it provides the function for maintiaining the secured state if there is a failure in the important process and a Repository.

- FPT_ITT.1
  This SFR corresponds to O.TSF data transfer protection since it provides the protection forinternally transmitted TSF data between the separated TOEs.

- FPT_STM.1
  This SFR corresponds to OE.TIME since it provides the reliable time stamp.

- FPT_TRC.1
  This SFR corresponds to O.TSF data transfer protection since it guarantees the consistency of internally copied TSF data.

- FPT_TST.1
  This SFR corresponds to O.TSF data protection since it provides the self test for TSF.

- FTA_SSL.1
  This SFR corresponds to O.Identification and authentication, O.TSF data protection since it provides the function of protection for the session during which a Security Administrator and a Security Client User access TOE.

6.3.2 Theoretical ground for The security the security assurance requirements

The the security the security assurance requirements in this ST accepts EAL4 the security the security assurance requirements.

EAL4 makes sure that a developer can acquire the maximum assurance from the practical security engineering based on the trustworthy commercial development methodology. The trustworthy commercial development is precise, but it does not require vast professional knowlege, technology, or other resources. EAL4 is the highest level at which it is economically feasible to update the existing production line.

EAL4 can be applied when a developer or a user requires the mid-to-high level of independently assuared security in the conventional TOE in use and when he is willing to pay additionally for the cost due to the security engineering.

In order to understand the security-related activities, EAL4 provides the assurance by analyzing the the security functional requirements included in a complete ST by way of a functional and complete interface specification, the instructions, the basic module design description of TOE, the expression of implementation for a part of TSF.

This analysis is supported by the independent test of TSF, the evidences in a test performed by a developer based on a functional description and a TOE design, the independent confirmation by test result sample, and the vulnerability analysis to prove the endurability from the intrusion of an attacker who possibly succeeds to do harm to the system in a reinforced or basic mode based on (provided functional description, TOE design, the expression of implementation, architecture design, and evidences in instructions).

The following table is the list of assurance documents of TOE corresponding to each assurance component.

[Table 6-10] Assuarance method list

Assuarance class	assuarance component		Assuarance methods
development	ADV_ARC.1	securityarchitecture description	Chakra Max Core v2.0 security architecture
	ADV_FSP.4	complete functional description	Chakra Max Core v2.0 function specification
	ADV_IMP.1	the expression of implementation for TSF	The expression of implementation of Chakra Max Core v2.0
	ADV_TDS.3	basic module-based design	Chakra Max Core v2.0 TOE design documentation
instructions	AGD_OPE.1	user operating instructions	Chakra Max Core v2.0 administratorinstructions Chakra Max Core v2.0 administratorinstructions Chakra Max Core v2.0 userinstructions
	AGD_PRE.1	preparation procedure	
life cycle support	ALC_CMC.4	production support, acceptance procedure and automation	Chakra Max Core v2.0 configuration management documentation
	ALC_CMS.4	the range of problem-	

		seeking configuration management	
	ALC_DEL.1	distribution procedure	Chakra Max Core v2.0 release procedure documentation
	ALC_DVS.1	The identification of security measures	Chakra Max Core v2.0 development security documentation
	ALC_LCD.1	life cycle model defined by a developer	
	ALC_TAT.1	Well-defined developer tool	
Security target specification assessment	ASE_CCL.1	Conformance claims	Chakra Max Core v2.0 ST
	ASE_ECD.1	Definition of expanded component	
	ASE_INT.1	Introduction to ST	
	ASE_OBJ.2	security target	
	ASE_REQ.2	derived security requirements	
	ASE_SPD.1	Definition of security problems	
	ASE_TSS.1	TOE summary specification	
Test	ATE_COV.2	Analysis of test-range	Chakra Max Core v2.0 Test documentation
	ATE_DPT.1	basic design Test	
	ATE_FUN.1	function Test	
	ATE_IND.2	independent Test : sample Test	
vulnerability assessment	AVA_VAN.3	concentrated vulnerability analysis	-

6.4 Theoretical ground for Dependency relation

6.4.1 Dependency relation of the security functional requirements

In this ST, dependency relation of each security functional requirements provided in CC is satisfied as follows:

[Table 6-11] Dependency relation of the security functional requirements

No.	security function component	Dependency relation	remarks
1	FAU_ARP.1	FAU_SAA.1 Potential violation analysis	4
2	FAU_GEN.1	FPT_STM.1 Reliable time stamps	41
3	FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	2 28
4	FAU_SAA.1	FAU_GEN.1 Audit data generation	2
5	FAU_SAR.1	FAU_GEN.1 Audit data generation	2
6	FAU_SAR.3	FAU_SAR.1 Audit review	5
7	FAU_SEL.1	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data	2 32
8	FAU_STG.1	FAU_GEN.1 Audit data generation	2
9	FAU_STG.3	FAU_STG.1 Protected audit trail storage	8
10	FAU_STG.4	FAU_STG.1 Protected audit trail storage	8
11	FDP_ACC.1	FDP_ACF.1 Security attribute based access control	12
12	FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	11 31
13	FDP_IFC.1(1)	FDP_IFF.1 Simple security attributes	18
14	FDP_IFC.1(2)	FDP_IFF.1 Simple security attributes	19
15	FDP_IFC.1(3)	FDP_IFF.1 Simple security attributes	20
16	FDP_IFC.1(4)	FDP_IFF.1 Simple security attributes	21
17	FDP_IFC.1(5)	FDP_IFF.1 Simple security attributes	22
18	FDP_IFF.1(1)	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	13 31
19	FDP_IFF.1(2)	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	14 31

20	FDP_IFF.1(3)	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	15 31
21	FDP_IFF.1(4)	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	16 31
22	FDP_IFF.1(5)	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	17 31
23	FIA_AFL.1	FIA_UAU.1 Timing of authentication	26
24	FIA_ATD.1	Not Available	-
25	FIA_SOS.1	Not Available	-
26	FIA_UAU.2	FIA_UID.1 Timing of identification	28
27	FIA_UAU.7	FIA_UAU.1 Timing of authentication	26
28	FIA_UID.2	Not Available	-
29	FMT_MOF.1	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	36 37
30	FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	11, 13, 14, 15, 16,17 36 37
31	FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	30 37
32	FMT_MTD.1	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	36 37
33	FMT_MTD.2	FMT_MTD.1 Management of TSF data FMT_SMR.1 Security roles	32 37
34	FMT_SAE.1(1)	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps	37 41
35	FMT_SAE.1(2)	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps	37 41
36	FMT_SMF.1	Not Available	-
37	FMT_SMR.2	FIA_UID.1 Timing of identification	28
38	FMT_SMR.3	FMT_SMR.1 Security roles	37
39	FPT_FLS.1	Not Available	-
40	FPT_ITT.1	Not Available	-
41	FPT_STM.1	Not Available	-

42	FPT_TRC.1	FPT_ITT.1 Basic internal TSF data transfer protection	40
43	FPT_TST.1	Not Available	-
44	FTA_SSL.1	FIA_UAU.1 Timing of authentication	26

6.4.2 Dependency relation of the security the security assurance requirements

Since in this ST, the assuarance package required in each assuarance requirement provided in CC part 3 is applied as it is, dependency relation is satisfied.

7 TOE summary specification

TOE summary specification describes simply and clearly how the security functions in TOE are implemented. Also it describes how the the security the security assurance requirements are satisfied.

7.1 TOE security function

This passage describes TOE security functions With regard to Chakra Max Core v2.0, a product for controlling DB access, it describes how TOE satisfies each security functional requirements specified in Chapter 6 of ST.

7.1.1 Security audit

Security audit consists of the functions of TOE in collecting the information on communication between the Protective DB and DB users and saving it in a repository, issuing the alert for the audit data violating the security policy, and protecting a repository. security audit mainly consists of the audit data creation, the audit review, and the protection of audit data repository. The description of each function is as follows:

7.1.1.1 Audit Data generation

The audit target events provided in TOE are as follow:

[Table 7-1] The audit data saving items by audit target event

Function component	Audit target events	Auditing target events provided from TOE	Auditing data storage category
FAU_ARP.1	Actions taken due to potential security violations.	when warning mail/warning SMS is sent	mail receiving address/SMS receiving telephone number
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms.	when login failure count is reached and the alert is issued	Security Administrator: date, account Name, ID, IP address, a warning action Security Client User: date, account Name, ID, group name, IP address, a warning

			action
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	Logging policy creation, in case of change, deletion	date, Security Administrator account Name, ID, IP address, the policy name before/after policy change, Assigned Systems, Assigned Users
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.	In case of access block by access control policy	date, Protective DBinformation, Security Client User information, whether a warning action, a warning mail or a warning SMS is issued.
FDP_IFF.1(1)	Decisions to permit requested information flows.	In case of SQL and DB access block by information flow control policy	date, Protective DB information, Security Client User information, whether a warning action, a warning mail or a warning SMS is issued.
FDP_IFF.1(2)	Decisions to permit requested information flows.		
FDP_IFF.1(3)	Decisions to permit requested information flows.		
FDP_IFF.1(4)	Decisions to permit requested information flows.		
FDP_IFF.1(5)	Decisions to permit requested information flows.		
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions.	When login failure count is reached	Security Administrator: date, account Name, ID, IP address, a warning action Security Client User: date, account Name, ID, group name, IP address, a warning action
FIA_UAU.2	Unsuccessful use of the authentication mechanism.	- In case of authentication failure of Manager/Client(password	Security Administrator: date, account Name, ID, IP address, warning action

	All use of the authentication mechanism.	error) - In case of authentication attempt of Manager/Client	Security Client User: date, account Name, ID, group name, IP address, a warning action
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	In case there is a failure in authentication of Manager/Client(user ID error)	Security Administrator: date, IP address, a warning action user: date, IP address, a warning action
FMT_SMF.1	Use of the management functions.	Registration, modification/deletion of Manager, Client,DB, Server	Date, Security Administrator account Name, ID, IP address, Security Administrator before/after the change, Security Client User, Protective DB, Protective Server information
		In case of creation, modification and Deletion of security policy/logging policy	date, Security Administrator account Name, ID, IP address, policy information before/after policy change, Assigned Systems, Assigned Users
		In case of setting and changing TOE environment variable	date, Security Administrator account Name, ID, IP address, environment variable setting value before/after change
		In case the limit value changes among TOE environment variables	date, Security Administrator account Name, ID, IP address, the environment variable limit setting value before/after change
		In case when there is a creation/change/deletionof a group of Manager/Client	Security Administrator: date, Security Administrator account Name, ID, IP address, group information before/after change Security Client User: date,

			Security Administrator account Name, ID, IP address, group information before/after change, Assigned Users
FMT_SMR.2	Modifications to the group of users that are part of a role. Unsuccessful attempts to use a role due to the given conditions on the roles.	When the group of Manager/Client is changed	Security Administrator: date, Security Administrator account Name, ID, IP address, group information before/after change Security Client User: date, Security Administrator account Name, ID, IP address, the group information before/after change, Assigned Users
FMT_SMR.3	Explicit request to assume a role.	When there is a request from a Client to delegate an Approver	date, Security Client User account Name, ID, IP address, delegate Security Client User name
FPT_STM.1	Changes to the time.	In case time of Manager/Client changes	Time before/after change
FPT_TRC.1	Restoring consistency upon reconnection.	In case there is an failure while Manager/Client work on update	date, TOE version
FAU_STG.3	Actions taken due to exceeding of a threshold.	In case that audit data storage space is insufficient (90% full)	date, Protective DBinformation, whether a warning action, a warning mail or a warning SMS is issued
FAU_STG.4	Actions taken due to the audit storage failure.	In case the space for saving audit data is exceeded (95% full)	date, Protective DBinformation, whether a warning action, a warning mail or a warning SMS is issued.

TOE collects the information on communication between the Protective DB or the Protective Server and DB user from the network stream, analyzes the packets, creates and combines the information on the Protective DB access and SQL log, and save it in a repository.

TOE collects the information on DB users' access to the Protective DB access and SQL information and provides it to a Security Administrator on DB Session Monitor in real time. It saves the audit data in a repository based on logging policy. Also, it saves and manages the newly generated SQL in each Protective DB in the individual table.

TOE collects the following information from a DB users' sniffing session and save it in a repository.

- OS type and version information
- OS Account
- DB Account
- use Application information
- user IP
- access Port
- SQLsentence information

Also, TOE collects the following information as a response of the Protective DB to DB users' sniffing access and saves it a repository.

- SQL performing result
  - response number
  - response result
  - error code and message

From a Security Client User's gateway session, TOE collects the following information and saves it in a repository.

- OS type and version information
- Security Client User account information
- OS Account
- DB Account
- use Application information
- user IP
- access Port
- SQL sentence information

Also, TOE collects the following information as a response of the Protective DB to Security Client Users' access and saves it in a repository.

- SQL performing result
  - response number
  - response result
  - error code and message

TOE provides a Security Administrator with alert data for the session and SQL of DB users who violate the security policy via Alert Ticker in Chakra Max Manager v2.0 in real time, informs a Security Administrator of the detail of violation selectively by SMS and E-Mail, the record and information of alerts in a repository.

Also TOE saves the audit data about the agenda for SQL approval between the Security Client Users, the approval information and the audit data about the record in a repository.

With regard to a Security Administrator's access to TOE, TOE creates the following audit data about operating TOE and saves it in a repository.

- TOE identification and authentication
- TOE environment setup
- Logging policy setup
- Alert policy setup
- Masking policy setup
- Approval policy setup
- TOE Update
- alert data when audit data loss is expected
- integrity examination error

With a Security Client User's access to TOE, TOE creates the following audit data of Security Client User and saves it in a repository.

- TOE identification and authentication
- Delegation of approval privileges to Approver on one's behalf

7.1.1.2 Audit review

Chakra Max Manager v2.0 provides a Security Administrator with various forms of functions for audit review. First, there is a session monitor with a screen on which the information on a DB user's session and SQL can be monitored in real time, Alert Ticker from which the alert issue can be checked in real time, and Alert Monitor for querying this. And it provides the audit review function by which the audit data and the alert data can be selectively queried according to the attribute. Selective audit is supported in Database audit log, Alert log, Approval log, a Security Administrator's Work History log, and a Security Client User's audit log.

- Session Monitor

Session Monitor is the function for providing the screen on which one can monitor in real time the information on the session during which a DB user access to the Protective DB and the efficiency and situation of SQL performed in each session.

On the screen on which he can monitor the Protective DB access session, a Security Administrator can query the current status of session access , the DB user information, the access application name, the information on performing SQL, and the alert situation, etc. Also, if he finds the unauthorized session and SQL, he can block the session in real time.

- Alert Ticker

Right below the toolbar of Chakra Max Manager v2.0, there is Alert Ticker which shows the alert situation of the unauthorized access to the Protective DB in real time.

Alert Ticker is not displayed when there is not a record of Alert generating situation, but if Alert occurs, it is shown. When one places a cursor on it, the brief information can be checked. When he clicks it, the detailed information is displayed.

On Alert Ticker, Alert(Unconfirmed Alert) not confirmed by a Security Administrator is shown. Once it is confirmed, it will be longer displayed.

- Alert Monitor

Alert Monitor provides the function with which to check Alert data created for user data protection as a coping action against the event violating the security policy and to analyze the cause.

Alert Monitor provides Alert Calendar in a calendar form, which lets you check Alert generating data and Unconfirmed Alert screen to show only Alert details not confirmed by a Security Administrator in a form of list. In Alert Calendar, you can check the Alert situations by the relevant date and time and can confirm the record of alert occurrences at a glance through the weekly and monthly calendar. Also, it is possible to query only the important alert separately, according to the importance of alert.

- Search

The audit data collected by TOE can be queried through the various search perspectives and search functions, and the function of detailed view into each data is provided.

Search provides the following functions.

- Database: it provides the search and the detailed record about all data of the audit performed in the Protective DB.

- Alert: it provides the search and the detailed record about the alert data violating the alert policy set by a Security Administrator.
- Approval: it provides the agenda by the policy of approval performed a Security Client User, the details of approval, the audit data and the detailed record about the history of performing SQL.
- Work History: it provides the search and the detailed record about the history of the startups or the changes, etc. of a security policy performed by a Security Administrator.
- Client: it provides the search and the detailed record about the use of TOE by a Security Client User.

Among Search functions, Database, Alert, Approval search conditions provide the function with which to adjust the screen for search condition entry by Simplified Search and Advanced Search.

7.1.1.3 Audit data repository protection

TOE informs a Security Administrator by Alert message of "Low Disk" when the audit data reaches 90% of capacity of a respository with a view to preventing the data loss of Repository used as an audit data saving space (by printing it out in Alert Ticker and sending SMS and E-Mail) and saves the alert data. And when audit data reaches 95% of a capacity, it notifies a Security Administrator by Alert message of "Full Disk" (by printing it out in Alert Ticker and sending SMS and E-Mail) and saves the alert data. Also until the space for saving the audit data in a Repository is secured to less than 95%, the security function is suspended temporarily and the record of the security function suspension is saved in File System.

Also, TOE blocks the remote access to a repository in order to prevent the unauthorized access to a repository or the change and deletion in a repository. Repository makes encrypted communication with TOE and all other accesses are blocked.

TOE backs up the audit data of Repository autonomously in order to secure space in a repository(default: once a day), and the backed up compressed files will be managed separately in File System. Also if necessary, the backed up files are recovered so that the audit data can be queried.

Chakra Max Backup can be periodically executed at scheduled time according to policy or it can be executed in real time by a Security Administrator.

7.1.1.4 Security alert

TOE generates Alert for the following events considered as the unauthorized access to TOE, the unauthorized to the Protective DB or the threat to TOE operation and it informs a Security Administrator of security threat by E-Mail and SMS and saves the relevant alert data in Repository.

- The Protective DB access by DB users who violates alert policy
- TOE access failure of a Security Administrator and a Security Client User
- The Protective DB access failure of DB users
- the Protective DB access due to the falsification of application name
- Insufficient capacity of Repository
- unusual shutdown of important processes of TOE
- Integrity error of TSF data
- New SQL occurrence in a sniffing session

7.1.2 User data protection

User data protection is divided into access control and information flow control. Access control assigns the Security Client Users by Protective DB and provides the function for blocking the access of Security Client Users without privilege to the Protective DB. Information flow control provides the function for partially controlling the information flow of DB users via Alert policy, Masking policy, Approval policy and NEW SQL policy.

7.1.2.1 Access control

- Access control by Protective DB

TOE manages Security Client Users by specifically designating those who can access each Protective DB. The group of Security Client Users assigned in each DB or each Security Client User is allowed to access the Protective DB, or otherwise other Security Client Users' access is blocked. Therefore the Security Client Users without access privileges are blocked from access to the Protective DB in advance before the security policy for information flow control is applied to them.

- Work Time SQL execution control

TOE provides Work Time control function to block the privileges for pre-approved in non working hours or on holidays.

A Security Client User can set up the constrainst on execution count for the relevant SQL when he drafts the SQL which will acquire the execution privilege for the Protective DB. He can execute

SQL up to this number without additional drafting. Then, if he set up the time for controlling Work Time for each Protective DB, he can execute the approved SQL only at the permitted time and at the interrupting time even the approved SQL cannot be performed.

However, for the continuity of the work, the approved SQL can be executed even at the interrupting time for Work Time, using the approval line designated as 'emergency approval'. Also through the emergency approval, the new draft can be approved.

- Security Client User IP control

TOE provides the function for restricting TOE access at a Security Client User's IP address. The security client IP controlling function blocks the login to Chakra Max Client v 2.0 from other PCs than at the permitted IP addresses for each Security Client User.

- Data Masking

TOE can provide a Security Client User with all the data masked with the asterisks '*' according to the policy type of Masking policy: in case of Full Masking, all the data in the column are masked with '*'. Also, in case of Partial Masking, only some data are maksed with "*" letters according to a format, with the data in the other remaining digits provided as they are.

7.1.2.2 Information flow control

TOE generates Alert according to Alert policy in order to control the unauthorized access to the Protective DB and perform the Reject SQL or Kill Session according to the attribute. Also it provides the important data to users as they are masked as a result of SQL execution. And in order to individually control Security Client Users it applies Approval policy and enhances the usefulness of security management by use of New SQL and Safe SQL.

- Alert

TOE provides Alert policy as a security policy for information flow control of the Protective DB. By using Alert policy, TOE can block DB users' session. For a Security Client User, individual Reject SQL is possible in addition to the Kill Session.

Information flow control method in Alert policy is as follows:

- No Protection (Alert Only)
- Kill Session
- Reject SQL

TOE performs control of the unauthorized access among DB users' sessions according to Alert policy and save the record of the performance in Repository.

Also TOE provides the function for applying the different control method at each level by rating the levels in Alert policy or for querying the alert data by level. Also, according to the set Alert Level, when there is an alert, it provides the function for sending E-Mail or SMS selectively to a Security Administrator.

Alert level is as follows:

- Critical
- Major
- Minor
- Warning
- Information

- Data Masking

TOE provides Data Masking Function, in which the resultant values are given after the important information is masked to a Security Client User who wishes to request the information of a Protective DB.

Also, TOE saves the history of performance of Data Masking in a Repository according to Masking policy

- SQL Approval

TOE provides SQL approval function via Approval policy in order to control the Protective DB access by SQL unit from a Security Client User who performs the unformatted SQL by accessing the Protective DB in a Gateway Mode.

Also TOE saves the record about performing SQL and of approval by Approval policy in Repository.

- New SQL control

TOE applies more moderate information flow control to DB users who execute a large number of formatted SQLs in the Protective DB in a Sniffing mode via the machines such as Application Serve or Web Server, etc., than to users who access to it in a Gateway Mode. However in this case, when New SQL against the pattern is executed, it can be considered that there is a hazard to make threat to the DB, so using New SQL Control policy, a DB user's information flow is controlled.

New SQL policy can generate Alert or respond to Kill Session according to attribute and SQL approved by a Security Administrator will not apply New SQL Control policy any longer

- Allowing Safe SQL

As TOE controls SQl individually for a Security Client User via Approval policy, security can be enhanced but the work convenience can be lowered. Accordingly, it provides the function of reducing the incovenience of work by not applying the security policy to a SQL basically generated when DB Client Tool is executed and to a safe and frequently used SQL

As for Safe SQL, a Security Client User who executes SQL makes a request for approval of Safe SQL to DBA, and the SQL approved by DBA will be delivered to a Security Administrator at the second phase. A Security Administrator can register SQL as Safe SQL in the list of Safe SQL registration requests or withdraw it from the list.

- Real time information flow control of DB user session

TOE provides the function for a Security Administrator to arbitrarily block the unauthorized access while DB user session is monitored in real time via DB Session Monitor.

7.1.3 Identification and authentication

7.1.3.1 Identification and authentication

A Security Administrator accesses TOE via Chakra Max Manager v2.0 program and manages the security function, and a Security Client User accesses the Protective DB via Chakra Max Client v2.0.

TOE secures the safe channel using SSL, and when a Security Administrator and a Security Client User log in to Chakra Max Manager v2.0 and Chakra Max Client v2.0 respectively, the identification and authentication is given through ID and password.

For access to TOE, TOE provides a Security Administrator and a Security Client User with the following items of login screen.

- ID: the account for access to TOE
- PW: the secret numbers of a Security Administrator account and a Security Client User account
- [Login] Button: When the button is selected, by checking the entered Security Administrator account and security client account and secret number, it authenticates and identifies the users and allows access to TOE.

When a Security Administrator or a Security Client User is authenticated, the secret number is substituted with the letter “*” so that the authentication feedback may be protected.

When a Security Administrator is identified and authenticated successfully, the session is created and it will take a user to the main screen on which he can access the audit and management screen. Also, when a Security Client User is done with the identification and authentication successfully, the session is created and it will take him to the main screen on which he can use the approval process.

A default value of Top-level Administrator account is not provided but it will created when Chakra Max Server v2.0 is installed. And, at this time, the IP address of a Top-level Administrator’s PC is also entered. On other PCs than at the permitted IP address, it is impossible to access TOE with a Top-level Administrator account. Also, a Top-level Administrator should never fail to change his password when he accesses TOE for the first time. Also, at an Security Administrator account registered by a Top-level Administrator, he is forced to change the password when the user accesses TOE for the first time after the creation of account creation.

When a Security Client User accesses TOE for the first time, he logs in with the password set by Security Administrator, but this should also be changed.

Also, the validity term for a Security Administrator account and a security client account can be set up. If this period is over, it is impossible to access TOE.

And the validity term for the secret number of a Security Administrator account and a security client account can be set up. From 7 days before the validity term of a secret number is over, TOE makes a request for change of the secret number to a Security Administrator and a Security Client User by messages. And when the validity term of secret number is over, it automatically makes a request for change of secret number to a Security Administrator and a security client. At this time, if the secret number is not changed, it is impossible to access TOE.

A Security Administrator ID and a Security Client User ID should be made with the letters shorter than 40byte.
A Security Administrator ID and a Security Client User ID should satisfy the following rules in case of secret numbe, even though there are no other special constraints than the rules above.

- English upper case A~Z (26 letters)

- English lower case a~z (26 letters)
- numeric 0~9 (10 letters)
- Special characters : `~!@#$%^&*()-_=+[]{}₩|;:‘’“”,.<>/? (34자)
- password combination rules
  - English letters + numeric + special characters combined
  - digit : 8 ~ 16
- passwords cannot be the same as IDs

TOE performs the following coping actions when there is a failure in processing the authentication.

- When there are failures in authentication from 3 to 10 times (default: 3 times) according as set by a Security Administrator, "authentication failure" message is displayed.
- When there are failures in authentication at more than the set count(default: 3 times), 'session lockup' is displayed for an amount of time set by a "Security Administrator (1 min.~43200 min.) with the record of audit left. And the re-authentication is prohibited for the amount of time.
- As authentication is made, if for the time set by a Security Administrator (1~1440 minutes; at default: 3 min.) there is no use of Chakra Max Client or Chakra Max Manager, the session is locked up and a Security Administrator and a Security Client User can use the system after their secret numbers are rechecked

In case of authentication success and session lockup due to authentication failure, the relevant information is saved as the audit data.

7.1.4 Security management

Security management consists of Logging policy, Protective Server, Protective DB, Alert policy, Approval policy, Masking policy, Safe SQL, New SQL Control policy, Work Time, Backup, Security Administrator, Security Client User, and TOE operating management function, and every function is managed in Chakra Max Manager v2.0. Each function plays a role as follows:

7.1.4.1 Logging policy management

TOE analyzes the packet information, saves and manages a huge amount of data in Repository. Also the audit data created while monitoring and logging is performed has the different sizes according to the Protective DB operating situation. For example, if the number in performing SQL operations per second is too large and if the performed SQL sentence is long, the information to be recorded becomes also much more. So, within a short period of time, the available disk space in Repository will run low. In other words, the operating policy is needed for enccouring users to highten the work efficiency in a variety of analyses through audit data by saving only the necessary information to effectively use the disk space.

Therefore, TOE provides Logging policy for the more effective management of disk space and audit data. A Security Administrator can establish Logging policy so that the audit data can be effectively created via the analyses into the characteristics of the Protective DB, the periodical change in the operating situation, and the tendency of DB users.

Generally speaking, a Logging policy provides the three attributes such as the operating time, the session information, and the type of performed SQL, etc., and only if each and every condition is satisfied, it saves the session information and SQL in Repository. The registered Logging policy can be activated or deactived depending on situation. If Logging policy is not individually managed, at default value it saves the access session information and the record of the performed SQL in all the Protective DBs monitored by TOE as the audit data.

7.1.4.2 Protective Server management

Protective Server management function is a function for managing the information on servers equipped with the Protective DBs and it can include the information on a number of IPs with a view to supporting IPs used by the duplexed DB Servers.

The registered Protective Servers can be activated or deactivated depending on the situation. The activation or deactivation of Protective Server has nothing to do with whether or not the Protective DB is activated.

Also, various kinds of Protective Servers are to be grouped and managed.

7.1.4.3 Protective DB management

Protective DB management is a function for registering the information on the Protective DB and the entry field is applied by the Protective DB type (Oracle/MySQL/MSSQL/Teradata/DB2/Tibero/Sybase ASE/Sybase IQ/Informix/Altibase).

The registered Protective DB can be activated or deactivated according to the situation and if activated, the Protective DB will not be controlled and inspected. But it is possible to query the previsoulsy saved audit data. However if the Protective DB is deleted, the audit data will also be deleted so it is impossible to make a query.

Also, various forms of Protective DBs are to be grouped and managed.

7.1.4.4 Alert policy management

Alert policy management function is a function for registering the security policy for Alert and the interrupting action to the unauthorized access to the Protective DB and for querying the current situation. Alert means a function for TOE's recognizing the problems in security or performance of the Protective DB and notifying a Security Administrator of them by Alert Ticker, E-mail or SMS.

TOE can provide the setting conditions by more than 20 combinations of various attributes and define the Protective DB to which Alert policy will be applied and the DB users.
Alert has the Alert level to express its severity. TOE provides 5 levels of Alert ranging from Critical, Major, Minor and Warning to Information, and a Security Administrator defines the appropriate Alert Level considering the characteristics of the settings in Alert policy. According to the situation in each Alert Level, a Security Administrator can take a coping action. Depending on the situation, he can set up the coping action by SQL block or session block. In addition, it provides a function for sending E-mail or SMS to a Security Administrator about the details of Alert.

- attributes of various alert policy setting functions
  - Date/Time: access date, access time
  - Connection: IP address, MAC address, Application name, Protective DB accountinformation, OS User name, computer name
  - SQL: SQL response time, SQL result line number, query size, response query size, SQL result code, SQL sentence (Type, Text, Command, Full Text) information, SQL command, Protective DB information (Table, Column), time of session not in use, SQL number, SQL result value, the number of recent SQLs, recent SQL transfer volume
  - Policy Item Group
  - Security Client User name, Security Client User group
  - Protective DB Name

- the attribute corresponding to Alert event
  - Only Alert: Alert is generated for session and SQL which violate Alert policy
  - Kill Session: session block action is performed for session and SQL which violate Alert policy
  - Rejected SQL: SQL block action is performed for session and SQL which violate Alert policy. However, it can be applied only in a Gateway Mode session

- Function for sending the details of Alert situation

- Sending E-Mail: It is possible to set up E-Mail address at which an alarm notice about Alert will be received in addition to a Security Administrator.
- Sending SMS: It is possible to set up a mobile phone number at which an alarm notice will be received in addition to a Security Administrator.

7.1.4.5 Approval policy management

TOE controls the direct access by a Security Client User to the Protective DB. It provides a approval function for allowing or blocking access using SQL approval. If regarding the use of Protective DB, a Security Client User with a low security privilege should acquire or change the important information of the DB, it can let him access the Protective DB using SQL approval. By doing so, it can have more flexible information flow control of a Protective DB. Approval function can be used as approval line management and Approval policy management.

Approval line management can designate the approval line used when a Security Client Users makes SQL approval, whether he can make pre-approval or post-approval, and whether he can make approval on one's behalf or emergency approval.

For approval routes on which approval on one's behalf is not allowed, only the originally designated Approver can make approval or denial, regardless of the delegation of approval right. The approval line for emergency approval is to be used when the emergency task should be processed even during the period for Work Time control.

Approval policy management function has a function for setting up the conditions on which a Security Client User can set Approval policy. Approval policy can be applied with policy priority set from 1class to 10class. 1class is the top priority. TOE can set the policy by flexibly combining various conditions of Protective DBs and Security Client User attributes.

Also, approval line suitable for Approval policy conditions can be set. Besides, it is possible to selectively set a Security Client User or the Protective DB to which the relevant Approval policy condition is to be applied.

In the time zone set for Work Time, approval is not to be performed. So, it is possible to set the emergency approval route for solving this problem.

7.1.4.6 Masking policy management

TOE provides a function for preventing a security information leak by masking the information in case data contains the information requiring security such as resident registration number, card number, or bank account number, etc. when a Security Client User wants to access the Protective DB for some data data. TOE provides a Security Client User who accesses the table containing the important information with data as partially or fully masked.

Masking policy management function provides Masking policy setup conditions with a variety of combinations of the following attributes and it can define the Protective DB to which Masking policy is to be applied and a Security Client User.

- Date/Time: access date, access time
- Connection: IP address, MAC address, Application name, Protective DB accountinformation, OS User name, computer name
- SQL: SQL sentence (Type, Text, Command, Full Text) information, SQL command, Protective DB information (Table, Column)
- Policy Item Group
- Security Client User name, Security Client User group
- Protective DB Name

Masking can set a full or Partial Masking policy by Table or Column unit for each Protective DB.
In Full Masking, maksed letters are shown for the digit-number of the data.

Example) If after setting a Full Making policy in "empno" column of "emp" table, one accesses the DB and retrieves the data, the following result will show up.

Data before masking	Data after masking
chakramax	********
chakramaxtest	***********

In Partial Masking, the data is shown as masked letters for the set digits.
Partial Masking supports only the character type of data column. The numeric type of data is to be fully masked. The form of Partial Masking is made by a combination of "*" letter and others. A portion of "*" is masked and the portions set with other chracters than "*" are not masked. Also, when the digit number of the actual data is fewer than the digit number in a form set by Masking policy, the data will be fully masked. On the other hand, when the digit number of the actual data is more than that in a form set by Masking policy, it will be fully masked regardless of the form.

Example) If after Partial Masking Format in Masking policy is set in a form of "**-**-**", one accesses the DB and retrieves the data, the following result will show up.

Data before masking	Data after masking
chakrama	**a**a**
chakra	******
chakramax	**a**a***

7.1.4.7 Safe SQL management

TOE has a high degree of security because it controls SQl individually by Approval policy for a Security Client User, but the convenience can be lowered. Therefore, for a Safe SQL basically generated when DB Client Tool is executed, it provides a function for enhancing a convenience by not applying a security policy which controls SQL.

Safe SQL management is a function for not applying a security policy to the SQL considered safe by a Security Administrator, such as the SQL basically executed when a DB Client Tool is executed. In case it is registered as a Safe SQL, a Security Client User can execute the SQL without any restriction.

Safe SQL is managed by the Protective DB Type. Uapproved Safe SQL requested by DBA of the Protective DB can be registered as a Safe SQL with the approval of a Security Administrator. Also it provides additional functions a Security Administrator can add manually.

The SQL not used for 30 days after it is registered as a Safe SQL will be marked in red letters to be left to the consideration of a Security Administrator about whether it is necessary or not.

7.1.4.8 New SQL management

New SQL management provides a function for changing a New SQL Control policy and querying and approving the generated New SQL.

A Security Administrator can set up whether New SQL it to be controlled by designating the period by the Protective DB. The types of New SQL control are Alert occurrence and session Kill.

7.1.4.9 Work Time management

Work Time management controls the Protective DB access by Approval policy. For the period set as the control time, it is possible to approve and access the Protective DB only through the emergency approval. The SQL approved and authorized not by emergency approval but by normal approval cannot be performed.

Work Time can be set by each Protective DB. It can be set from Monday to Sunday, by holidays or by time zones.

7.1.4.10 Backup management

TOE provides a backup function for TSF data and audit data. Since a huge amount of audit data is saved, Repository can be effectively utilized by Backup. If one wants a query of the deleted audit data, he can recover, query and analyze it from Backup.

TOE provides Daily Backup function at default. Backup process can be automatically executed by Backup management or it can manually operated by a Security Administrator by date.

By Backup management, a Security Administrator can set when Backup is implemented or time of operation, or he can set the directory of File System in which Backup files are created. Also for the audit data Backup of which is done, he can set the period(days) while it is kept in Repository. According to Backup success or failure, it is possible to select whether it will provide a Security Administrator with E-Mail notification service.

7.1.4.11 Security Administrator management

TOE can utilize all its management functions when Chakra Max Server v2.0 is installed and will create an account in which to register a Security Administrator. Via a Top-level Administrator, it can add, delete or change a new Security Administrator account but cannot delete this Top-level Administrator account

TOE can manage a Security Administrator by various roles. Role can have various options for the privilege by which a Security Administrator can manage or monitor a part of security functions. However, a Security Administrator management function is only allowed to a Top-level Administrator but a privilege of Security Administrator management cannot be granted to other roles.

Via a Security Administrator management function, a Top-level Administrator must register E-mail and SMS number at which a Security Administrator can receive Alert alarm message. Besides, by setting up the IP address of a Security Administrator computer, it forces a Security Administrator to limit an allowable IP address at which he can access TOE. Furthermore, it provides a function for setting a validity term of a Security Administrator account so that a Security Administrator account with the expired validity term cannot access TOE. Also, it assigns the Protective DB to be managed by each Security Administrator, so that it can restrict a Security Administrator from monitoring a Protective DB beyond his privilege.

Also, a Security Administrator can query and change his own information through Monitor -> Overview at Toolbar on screen. A Security Administrator can set up a secret number, a telephone number, a mobile phone number, an E-Mail address, a Alert Call Level, or whether he wants to receive SMS or E-Mail in his account.

7.1.4.12 Security client user management

TOE provides a function of Security Client User account management. Security client users can be managed by group for setting the privilege to access the Protective DB.

A Security Client User has the following roles

- DBA: A Security Client User having a privilege who can tune up a SQL and approve Safe SQL. Some of Root users can be appointed as a Security Client Users.
- Root: A Security Client User who has the privilege to access to the Protective DB using Chakra Max Client v2.0.

A Security Client User must have more than a Security Client User group. It is possible to set up the Protective DB to be accessible by Security Client User group or set the security policy to be applied Also, it provides a function for setting a validity term of a Security Client User account so that a Security Client User account with the expired validity term cannot access TOE.

In addition, a Security Client User can query and change his own information using Chakra Max Client v2.0. On my information screen in his account, a Security Client User can set up his secret number, telephone number, E-Mail address, Approver on his behalf, the period of approval on his behalf.

7.1.4.13 TOE operating management

Chakra Max Manager v2.0 provides a management function for checking and changing the operating environment setup information for Chakra Server. Also, it provides a function for starting up or suspending the engine of TOE.

The TOE operating setup value is registered as recommended when TOE is installed. A Security Administrator can modify this value for operation

7.1.4.14 Update management

Chakra Max Server v2.0 is manually updated by an administrator. Before update, it inspects the integrity of files and if the integrity is not valid, update is not processed. Also after update, it inspects the integrity of TSF data and if it is not valid, a security function is not restarted.

Chakra Max Manager v2.0 and Chakra Max Client v2.0 are automatically updated at the login by the encrypted communication (SSL) with Chakra Max Server v2.0. When update for Chakra Max Manager v2.0 or Chakra Max Client v2.0 is requested, Chakra Max Server v2.0 performs the audit of the integrity of update files located in the specific directory. If Update files do not pass the integrity audit, TOE will not download the update files. Also, if after the download of update files the size of update files is not valid compared before the download, TOE will not process update. In addition, after Update is done and if the integrity of TSF data is not valid, it will not provide a security function.

TOE saves the time and the details of Update success and failure and TOE version information in File System.

7.1.4.15 Policy Item Group management

TOE can manage the main attributes of DB users, such as Client IP Address, Database Account, Application name, Security Client User, Table in Protective DB, and Column information in Protective DB, as Policy Item Group and can use them in the security policy.

7.1.4.16 Delegation of Approver role

TOE provides a function for delegating Approver roles of a Security Client User with a view to making work flow smooth in absence of a Security Client User having Approver privilege. A Security Client User to whom approval roles are delegated for a set period is granted all approval privileges from a role-giver. If this period is over, the roles will be automatically returned to a role-giver.

7.1.5 TSF protection

Chakra Max inspects the integrity of important TSF data when process is in operation and when a Security Administrator requests.

7.1.5.1 Verification of TSF data integrity

Integrity audit is processed in a way of comparing the hash value saved at the time of creation of TSF data with the currently entered hash value..

TOE leaves the record of audit when the executable files have the defects in their integrity and informs a Security Administrator by E-Mail and SMS. Until the problem is solved, it will suspend a security function temporarily. Additionally after a Security Administrator recovers it with safe TSF data, reoperates TOE engine and verifies the integral TSF data, a security function will operate normally.

7.1.5.2 Reliable time stamp

In order to provide the reliable time stamp, TOE synchronizes the time of a local computer with that of Chakra Max Server v2.0 at logins of Chakra Max Manager v2.0 and Chakra Max Client v2.0 programs and once per 5 minutes.

7.1.5.3 Health Check

TOE supports Health Check function for main processes in order to protect TSF data, examine the normal audit and keep user data protection. The record of Health Check is to be saved in File system of Chakra Max Server.

TOE suspends a security function when the main processes have some problems or terminated in an unusual way. Also, in this case, it will inform a Security Administrator by E-Mail. In addition, when faulty processes get back to normal, it will restart a security function automatically.

7.1.5.4 Reliable encrypted communication

Data communication between Chakra Max Server v2.0 and Charka Max Manager v2.0, between Charka Max Server v2.0 and Chakra Max Client v2.0, and between Chakra Max Manager v2.0 and Repository is encrypted with reliable SSL communication to keep integrity and confidentiality.

7.1.6 TOE Access

TOE leaves the special record about a Security Administrator's and a Security Client User's access to TOE. Also, if during the login process of Chakra Max Manager v2.0 or Chakra Max Client v2.0 program, there is not an interface for a time set by a Security Administrator (default: 3 minutes), it will lock up the session and require re-authentication.

7.1.6.1 Record of Security Administrator access

TOE saves the record of TOE access and TSF data change by a Security Administrator in Repository

7.1.6.2 Session protection

TOE provides the following setup functions in order to protect the sessions of a Security Administrator and a Security Client User.

- The cyle of Secret number change
- Login is prohibited for a period of time when there is an error in secret number
- Account is automatically locked up if there is no login activity for a period of time.
- Session is locked up if there is not an interface
- Secret number initialization value

A Security Administrator can limit the conditions on which a Security Administrator and a Security Client User must change their secret numbers after a period of time (default: 3 days) in a way of setting up a secret number change cycle. If there is errors occurring as many times as a secret number error coun t(default: 3 times) and basic error count, he can lock up the account so that the authentication may not be possible in minutes (default: 10 minutes) He can lock up the account to which one has not log in for a period of time (default: 30 days). In addition, the setup conditions are provided on which for the session not used for a period of time (default: 3 minutes), a function can be used only after one enters the secret number into the system again.

7.2 The rationale of TOE security functions

The rationale of TOE security functions proves the following items.

Each TOE security function is handled by at least more than one security functional requirements and each security functional requirements handles at least more than one TOE security function.

[Table 7-2] The rationale of TOE security functions

security function class	the security functional requirements	TOE security function
Security audit	FAU.ARP.1	Security alert
	FAU.GEN.1	Audit data creation
	FAU.GEN.2	Audit data creation
	FAU_SAA.1	Identification and authentication
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Audit review
	FAU_SEL.1	Logging policy management
	FAU_STG.1	Audit data repository protection
	FAU_STG.3	Audit data repository protection
	FAU_STG.4	Audit data repository protection
User data protection	FDP_ACC.1	Access control
	FDP_ACF.1	Access control
	FDP_IFC.1(1)	Information flow control
	FDP_IFC.1(2)	Information flow control
	FDP_IFC.1(3)	Information flow control
	FDP_IFC.1(4)	Information flow control
	FDP_IFC.1(5)	Information flow control
	FDP_IFF.1(1)	Information flow control
	FDP_IFF.1(2)	Information flow control
	FDP_IFF.1(3)	Information flow control
	FDP_IFF.1(4)	Information flow control
	FDP_IFF.1(5)	Information flow control
Identification and authentication	FIA_AFL.1	Identification and authentication
	FIA_ATD.1	Identification and authentication

	FIA_SOS.1	Identification and authentication
	FIA_UAU.2	Identification and authentication
	FIA_UAU.7	Identification and authentication
	FIA_UID.2	Identification and authentication
Security management	FMT_MOF.1	Security management
	FMT_MSA.1	Security management
	FMT_MSA.3	Security management
	FMT_MTD.1	Security management
	FMT_MTD.2	Security management
	FMT_SAE.1(1)	Security Administrator management, Security Client User management
	FMT_SAE.1(2)	Security Administrator management, Security Client User management
	FMT_SMF.1	Security management
	FMT_SMR.2	Security Administrator management, Security Client User management
	FMT_SMR.3	Delegation of Approver role
TSF protection	FPT_FLS.1	Health Check, audit data repository protection
	FPT_ITT.1	Reliable encrypted communication
	FPT_STM.1	Reliable time stamp
	FPT_TRC.1	Update management
	FPT_TST.1	TSF data integrity verification
TOE Access	FTA_SSL.1	Identification and authentication

6F, Nuritkum Square R&D Tower,
1605 Sangam-dong,
Mapo-gu, Seoul, Korea

FAX	+82-2-743-4912
SALES	purchase@warevalley.com
Partner	global@warevalley.com
Tech. Support	techsupport@warevalley.com