Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Security Target

Version:	**3.9**
Status:	**Final**
Last Update:	**2010-08-19**

Trademarks

Oracle and the Oracle logo are trademarks or registered trademarks of Oracle Corporation in the United States, other countries, or both.

The following terms are trademarks of Oracle Corporation in the United States, other countries, or both:

- Oracle Enterprise Manager Grid Control
- Oracle Management Server
- Oracle Application Server
- Oracle Database
- Oracle Enterprise Linux

The following terms are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both:

- Java

The following terms are trademarks of Red Hat Network in the United States, other countries, or both:

- Red Hat Enterprise Linux

The following terms are trademarks of SuSE Corporation in the United States, other countries, or both:

- SuSE Linux Enterprise Server

Other company, product, and service names may be trademarks or service marks of others.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
0.1	2008-11-05	Ochel, Powell	Created as part of the EMGC Readiness Assessment.
0.2	2009-02-20	Huynh	First draft for review
0.3	2009-02-25	Huynh	Incorporated developer's feedback
0.4	2009-04-01	Huynh	Incorporated developer's feedback including complete listing of all privileges in the TSS and in FDP_ACF.1, removed all AES references, clarified definition of agent and registration passwords, clarified SYSMAN/SUPER_USER role, added list of supported agent hosts in the TOE physical boundary, expanded the required setting of the evaluated configurations; and completed TSS

Revision	Date	Author(s)	Changes to Previous Revision
1.0	2009-04-02	Huynh	Fixed Figure 1 display.
2.0	2009-05-21	Huynh, Chapman	Fixed O.Auditing, O.ObjectAccess, O.UserAuth, and O.CompManage mappings to SFRs. Cleaned up unresolved dependency rationale. Fixed misspellings. Added FDP_ACC.1b, FDP_ACF.1b, FDP_ITT.1, FMT_MSA.1b, FMT_MSA.3, FPT_ITT.1. Removed FTP_ITC.1. Added T.Mask and modified O.UserAuth. Reworded FDP_ACF.1.1a. Revised TOE Overview. Reworded access control description for non-view privileges. Revised definition of agent keys, agent registration passwords, and brokered password. Added more details for crypto services. Removed agent hosts from physical boundaries. Added FPT_TDC.1 to cover crypto keys imported from the OS of OMS. Reworded SFR dependency rationale for FCS_COP.1. Fixed typos in FPT_TDC.1.
2.1	2009-05-26	Huynh	Started addressing certifier's comments.
2.2	2009-06-03	Huynh	Changed agent/target hosts to Linux platforms.
2.3	2009-10-20	Huynh	Added specific versions of OS platforms; Addressed certifier's comments; added A/OE KeyProtect and TargetAdmin, updated crypto key sizes; removed claim against secure comm. between agents.
2.4	2009-11-06	Huynh	Revised FAU_SEL.1 and FMT_MSA.1b. Revised crypto-related SFR's and their rationales to address certifier's comments. Removed TLS claims; Added FCS_CKM.1 for SSLv3 symmetric key and secret generation. Added AES claims.
2.5	2009-11-12	Huynh	Removed random number generation claims. Added an application note in FDP_ACF.1.2 to clarify the meaning of group to address evaluator's comment. Clarified details of agent/OMS authentication in the TOE description and TSS and the related SFRs. Removed VIEW_ANY_REPORT since it was determined not to be a supported privilege.
2.6	2009-11-13	Huynh	Addressed evaluator's comments.
2.7	2009-11-17	Huynh	Addressed evaluator's comments. Changed SFP in FMT_MSA.1b/MSA.3b back to Privilege-Based Access Control. As a result, added agent and OMS as subjects in FDP_ACC.1a/ACF.1a.
2.8	2009-11-19	Huynh	Addressed evaluator's comments. Clarified operator request in FDP_ACC.1a
2.9	2009-12-09	Huynh	Removed claims for selective audit (FAU_SEL.1).
3.0	2009-12-15	Huynh	Added EM_MONITOR privilege. Combined FMT_MSA.3a and FMT_MSA.3b into FMT_MSA.3 to remove redundancy. Removed agent/OMS security attributes from FDP_ACF.1. Added A.TargetSystem and OE.TargetSystem and updated related tables.
3.1	2009-12-16	Huynh	Updated FMT_MTD.1 - changing SUPER USER role to administrator-defined roles that contain OPERATOR_TARGET privilege.
3.2	2009-12-21	Huynh	Replaced authorized users with authenticated users wrt to audit review.
3.3	2010-01-08	Huynh	Removed claims for RSA key length 4096 bits.
3.4	2010-01-22	Huynh	Added reference to the ECD Guide. Corrected spelling errors.
3.5	2010-01-25	Huynh	Addressed evaluator's comments - added information about delivery method for patches.
3.6	2010-03-01	Huynh	Addressed evaluator's comments. Added patch 9019231.
3.7	2010-03-08	Huynh	Revised delivery method for guidance documenation
3.8	2010-05-26	Huynh	Addressed BSI comments - revised privilege definitions in TSS to be consistent with ECD; added clarification about crypto keys in TSS.
3.9	2010-08-19	Huynh	Clarified TOE delivery method.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Security Target
Version:	3.9
Status:	Final
Date:	2010-08-19
Sponsor:	Oracle Corporation
Developer:	Oracle Corporation
Certification ID:	BSI-DSZ-CC-0621
Keywords:	Oracle, EMGC, OMS

1.2 TOE Identification

The TOE is Oracle Enterprise Manager 10g Grid Control Release 5 Version 10.2.0.5.

1.3 TOE Overview

Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), or EMGC for short, is an enterprise management software solution. It provides administrators with access to network management functions through either web-based or command-line interfaces. With either of these, performance and health measurements of managed network systems can be queried, configuration of remediation policies can be edited, and routine tasks can be automated. Please note that the TOE will be referred to as EMGC for the remainder of this document.

EMGC implements Oracle Management Server (OMS), a web application server which provides the users with interfaces to the EMGC to manage remote hosts and applications (targets) as well as to view system measurements including diagnose performance and health issues of the target systems.

1.3.1 TOE type

Oracle Enterprise Manager Grid Control is a distributed software application that provides a centralized, integrated framework for managing other products in an enterprise grid. Management functionality includes performing software installation, patching, upgrading, workload balancing on the products that EMGC manages. The aspects evaluated are software components of the EMGC product along with the guidance documentation associated with the product.

1.3.2 Required non-TOE hardware and software

The non-TOE hardware and software needed by the TOE consist of operating systems for hosting the respective agents, targets, and CLI, in addition to the Oracle Application Server for the OMS, Oracle Database for the repository.

1.3.3 Intended method of use

The TOE employs a distributed architecture intended to be operated in a protected network environment. Other specific requirements for operating the TOE in the evaluated configuration are described in section 1.4.3.3.

1.3.4 Major security features

Security functionality provided by the TOE includes provision of authentication of users using the OMS-provided GUI and CLI interfaces to administrate remote targets; enforcement of access control in which users are granted with certain privileges to access managed objects; provision of transport layers for network communications between the remote parts of the TOE including secure communications between the OMS and the agents; management of security compliance of managed targets; management of the TOE's security functions; and auditing of security-relevant events.

1.4 TOE Description

1.4.1 TOE architecture

1.4.1.1 Overview

Oracle Enterprise Manager Grid Control (EMGC) is an enterprise management software solution that provides network management functions including to query performance and health measurements of managed network systems, edit configuration of remediation policies, and automate routine tasks.

The TOE is especially capable of managing databases in the network.

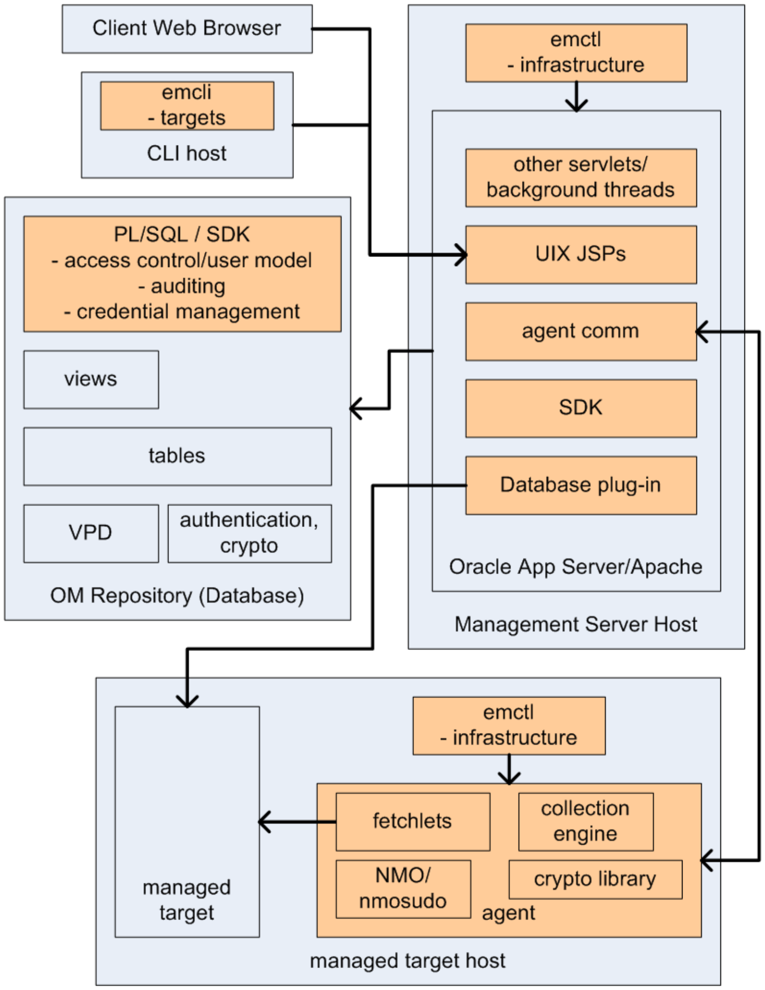

Figure 1: TOE architecture and boundary (orange components are part of the TOE)

Figure 1 presents an architectural overview of an EMGC deployment, illustrating the various components that comprise the TOE (orange/dark-shaded boxes) and its IT environment (blue/light-shaded boxes). Arrows are used to generally indicate information flows/connectivity between components (e.g., an arrow pointing from component A to component B would indicate that component A initiates communication with component B).

As seen in the Figure 1, the Oracle Enterprise Manager Grid Control is consisted of three major components: the Oracle Management Server (OMS), remote agents installed on the hosts of managed applications ("targets"), and an Oracle Database that serves as a repository of management information for the TOE.

Oracle Management Server

The Oracle Management Server (OMS) provides the TOE user with web-based and command-line interfaces to manage and control the TOE and the systems that it manages, and most, if not all, of the interaction between the user and the TOE take place through the OMS. Because of this, the OMS is central to the control of the entire TOE. The functionality of the OMS application is implemented within the Java-based Oracle Web Application Server. This application provides the communication mechanisms with agents and with the repository, serves the web-based interface with the help of an Apache server, and surfaces an SDK on which the TOE may be utilized and extended through the use of plug-ins.

The OMS web interface allows TOE users to view system measurements and perform management tasks. System measurements are provided by agents or plug-ins communicating with targets, and can be used to monitor activity and diagnose performance and health issues of managed systems. Tasks such as system provisioning, remotely installing updates and patches, adjusting system configuration, and performing maintenance actions can all be manually run or automated to run regularly.

Inside the OMS, an SDK is surfaced which allows the user or third-party software vendors to further extend the OMS functionality through plug-ins. A plug-in can give the OMS the specific knowledge it needs of a product to be managed allowing the TOE to perform customized direct management actions on that product, without the need of a remote agent. For example, in the evaluated configuration of the TOE, a database plug-in is installed that can perform direct database queries and commands, allowing the TOE user to create and schedule database maintenance commands and collect customized information about the database.

Agent/Target

The TOE has the ability to manage a wide variety of remote hosts and applications, referred to as targets. A target could range anywhere from a central database or server in a network infrastructure to a user's workstation. In order to perform remote actions within a managed network, each managed target has an agent that is installed to facilitate the management actions of the OMS. This agent communicates with the OMS to receive instructions which it then executes on the target. Monitoring and collecting credentials, for example user name and password needed to execute commands in a managed database, are stored by the agent on the target host. Host credentials are passed to the target's operating system for identification and authentication when requesting management actions on the operating system level. Details of agent/target are further explained in section 1.4.2.

Agents communicate over the network with the OMS via HTTPS in order to receive commands and deliver target information.

Repository

Data collected by the agents as well as a large amount of TOE configuration information is stored in the repository, which is implemented by an Oracle Database. The repository is used to host and execute a number of OMS-provided PL/SQL packages. Also, EMGC uses the repository as an authentication provider: the repository provides decisions on authentication requests that are then enforced by the OMS. Access control to objects held in the repository is partially implemented by the repository itself, using the Database-provided Virtual Private Database (VPD) and View mechanisms to restrict read access to authorized users, and partially by EMGC.

Access control for operations other than viewing database content is enforced with the help of explicit checks for privileges in the SDK access functions. Privilege checking is implemented by the PL/SQL scripts which simply check the access control lists to allow or deny the authenticated user from performing requested operations on defined objects.

1.4.2 TOE security function (TSF) summary

1.4.2.1 Identification and authentication

The primary TOE users are human users (administrators) using the TOE to administer remote targets, as well as the TOE itself. They have a unique user ID and access the TOE via the OMS-provided GUI and CLI interfaces. The TOE receives authentication credentials from these users and hands them to the repository in the IT environment, which returns an authentication decision. This decision is then enforced by the TOE by granting or rejecting access to the user.

The TOE performs authentication in other areas as well:

- agent registration passwords: passwords that can be defined by administrator and provided to agents for use during installation (bootstrapping). When a new, otherwise unknown agent registers with the OMS, the OMS will verify that the agent provides a valid registration password.
- agent keys: passwords defined for individually identified agents that are both stored in the OMS as attributes of the respective agent, and on the target host as part of the agent configuration. These passwords are negotiated during agent registration process. In other words, when the communication between the OMS and an agent is established, both ends verify that the HTTPS headers exchanged between them contain this password. Upon successful verification, the OMS generates the server certificate along with associated CA's and trusted certificates for the agent to download. The agent then uses that certificate to establish secure communications with OMS.
- Afterwards, when a connection is made between the agent and another entity (i.e. OMS), that entity may authenticate itself by participating in a challenge response with the agent. This verifies to the agent that the entity's private key corresponds to the public key in the OMS certificate that the agent has before.'

1.4.2.2 Privilege-based access control

Access control is enforced for administrator access to the TOE. The TOE implements a privilege-based access control mechanism, where users can be granted certain privileges (related to either the management of the EMGC system itself or targets managed with EMGC's help). EMGC's PL/SQL packages are used to determine whether requests for operations on objects (targets defined in the repository as well as other EMGC-related objects stored in the repository) are granted or not. An exception is the "View" privilege, where the TOE relies on Database mechanisms in the IT environment to enforce read access to objects in the repository. This is implemented by using the Virtual Private Database technology provided by the Oracle Database as well as the definition of Views in the database.

Privileges which give the administrator rights to perform management functions within EMGC can be grouped into roles that can be assigned to users. Targets can be grouped into target groups, and privileges can be associated with a group instead of with individual targets. The breadth of management tasks available in EMGC depends on the privileges and roles assigned to the administrators.

1.4.2.3 Auditing

OMS provides the central generation of audit records for security-related events, which are then stored in the repository. Actions simulated by users cause audit records to generate. The security-relevant events that get audited include the following:

- authentication attempts
- user login/logout
- management of users and their associated security attributes
- job management
- file transfer
- remote operations

In addition, each generated audit record includes event date and time, event type, user ID, event outcome as well as name and IP address of user's host machines.

1.4.2.4 Protected data transfer

Communication between the remote parts of the TOE is protected by encryption layers. The agents use the Oracle Crypto Libraries for SSL, a FIPS 140-2 compliant cryptographic module, to implement SSL for communication with the OMS host and the agents. Other parts of the TOE rely on the environment for the implementation of secure communication: OMS uses the facilities provided by the Web Application Server to establish the OMS-side of SSL tunnels, and to communicate with Databases (the repository as well as target databases) via net-ASO, a protocol to encrypt SQL traffic. Apache (provided by the IT environment) implements HTTPS for EMGC's web-based GUI.

1.4.2.5 Compliance management

EMGC offers functionality to compare the configuration of managed targets, such as security-relevant configuration settings, against administrator-defined policies (baseline configurations). Administrators can generate reports on and be notified about compliance violations.

1.4.2.6 Security function management

Administrators are offered management functions for the TOE's security functions, such as user and access control management, the configuration of the audit system, and the definition of security policies for targets.

1.4.3 TOE boundaries

1.4.3.1 Physical

The TOE is comprised of the following which is shipped on DVD media or downloaded electronically from Oracle's website:

- Oracle Enterprise Manager Grid Control 10.2.0.5 (DVD or electronic download)
- Oracle Enterprise Manager Agent (electronic download only) for one of the target host platforms specified below
- Oracle patches 8968670, 8814764, and 9019231 (electronic download only) which must be applied to the TOE after it has been installed.

The TOE also includes the following guidance documentation which is available for electronic download via the Oracle's website:

- Oracle Enterprise Manager Grid Control Online Documentation Library 10g Release 5 (10.2.0.5)
- Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)

The runtime environments for the different parts of the TOE are defined as follows:

- target hosts:
    - Oracle Enterprise Linux Version 4 Update 5
    - Red Hat Enterprise Linux AS Release 5
    - SuSE Linux Enterprise Server 10 SP1
    - Java Runtime Environment 1.4.2
- OMS:
    - Oracle Application Server 10.1.2.3
- repository:
    - Oracle Database 11g Release 1 (11.1.0.7)
- command line interface hosts:
    - Oracle Enterprise Linux Version 4 Update 5
    - Red Hat Enterprise Linux AS Release 5
    - SuSE Linux Enterprise Server 10 SP1
    - Java Runtime Environment 1.4.2

The operating system platforms listed above have been Common Criteria certified at assurance level EAL4 with [CAPP] compliance. Likewise, the Oracle Database listed above has been Common Criteria certified at assurance level EAL4.

Other IT products in the EMGC environment are:

- the managed targets, i.e. Oracle Database and Real Application Cluster instances
- web browsers used to access the web-based GUI provided by OMS
- an Apache web server on the OMS host

1.4.3.2 Logical

The security functionality provided by the TOE has been described above. The TOE relies on the IT environment for the provision of security functionality as follows:

- Target host (operating system):
    - The operating system hosting the managed target and agent(s) must restrict access to the agent and agent configuration data to authorized users.
- OMS host (Oracle Application Server):
    - The application server needs to protect the EMGC application, its configuration and other data against unauthorized access. It needs to provide a secure network connection to the repository and managed targets. The web server used to serve the web-based GUI to administrators needs to provide SSL-protected communications to remote users. Additionally, the IP address of the client machine (which is included in the audit records) is calculated by the OMS machine.
- Repository (Oracle Database):
    - The database needs to provide authentication decisions to OMS, VPD and other mechanisms to restrict access to the EMGC data stored in the database, and encryption of communication with the OMS. The database must restrict access to EMGC code and data, including audit records, to authenticated users. Additionally, it needs to provide a reliable time source for audit record creation.

1.4.3.3 Evaluated configuration

The following configuration specifics apply to the evaluated configuration of the TOE:

- SSL must be enabled for network communications in secure-lock mode.
- The only supported targets in the evaluated configuration are Oracle Database and target hosts identified above. The support for Oracle Application Server and Collaboration suite is not included in this evaluation.
- Audit must always be turned on
- For configuration of systems, EMGC 10.2.0.5 Security best practices should be used and Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) must be used.

1.4.4 Security policy model

The following is a list of the subjects and objects participating in the security policies defined by the SFRs for the TOE.

1.4.4.1 Subjects and their security attributes

- processes (users are represented by operating system processes. Operating systems use the user ID of a user to associate that user with the processes acting on behalf of that user)
    - user ID
    - privileges granted to the user
    - roles assigned to the user
- agent
    - identifier
    - agent password
- OMS
    - X.509 certificates

1.4.4.2 Objects and their security attributes

- database elements
    - object identifier
    - group membership (if object is a target)
    - privilege propagation group membership (if object is a target or member of a group)

1.4.4.3 TSF data

- subject and object security attributes
- audit records
- TOE configuration data
- target configuration baselines
- target "preferred credentials"
- X.509 certificates (public key certificates and private keys)

1.4.4.4 User data

- target configuration settings
- target information collected by the TOE

2 CC Conformance Claim

This ST is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL4, augmented by ALC_FLR.3.

This ST does not claim conformance to any Protection Profile.

Common Criteria [CC] and Common Evaluation Methodology [CEM] version 3.1 revision 3 have been taken as the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

The **assets** to be protected by the TOE are information stored, processed, and/or transmitted by the TOE. The term "information" is used here to refer to all data held within the product.

The **threat agents** having an interest in manipulating the data model can be categorized as either:

- Unauthorized individuals (“attackers”) which are unknown to the TOE and its runtime environment.
- Authorized users of the TOE ("i.e., administrators) who try to manipulate data that they are not authorized to access.

Threat agents originate from a well managed user community within an organizations internal network. Hence, only inadvertent or casual attempts to breach system security are expected from this community.

TOE administrators, including administrators of the TOE environment, are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Hence, only inadvertent attempts to manipulate the safe operation of the TOE are expected from this community.

3.1.1 Threats countered by the TOE

T.User

An attacker may able to gain access to the TOE without being properly authenticated.

T.Access

An unauthorized or authorized user may gain access to managed objects stored in the OMS without proper authorization.

T.Auditing

Security-relevant activities of unauthorized users (e.g. password change) and of authorized users (e.g., remote operations) may go unnoticed.

T.Compromised

Data transmitting between remote parts of the TOE may be compromised by an unauthorized or authorized user.

T.Compliance

Deviations of configurations of the systems the TOE manages ("managed targets") or compliance violations made by authorized or unauthorized users may go undetected.

T.Inactive

A user may gain unauthorized access to an interactive session after a period of inactivity.

T.Mask

A user may gain unauthorized access by viewing users entering their passwords during the authentication process.

T.TSFDataCom

An authorized or unauthorized user may compromise the TSF data (i.e. X.509 certificates used for SSL communications between the OMS and the agents) that are shared between the TOE and the trusted underlying operating system of the OMS.

3.2 Assumptions

3.2.1 Intended usage of the TOE

A.InstallConfig

It is assumed that the TOE is installed, configured, and operated in its evaluated configuration as defined in this Security Target and the TOE guidance.

3.2.2 Environment of use of the TOE

A.Physical

It is assumed that the machine(s) providing the runtime environment for the TOE, and the database for the OMS Repository, are protected from physical access and modification.

A.Admin

It is assumed the administrators of the TOE and of the operational environment are not careless, willfully negligent, or hostile. They are well trained and follow the administrator guidance properly to securely and trustworthy administer all aspects of the TOE operation mandated by this Security Target.

A.SelfProtect

It is assumed that the machines providing the runtime environment for the TOE are used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the operational environment.

A.KeyProtect

It is assumed that the X.509 certificates used for securing communications between the OMS and the agent are imported from the TOE's runtime environment. It is also assumed that such runtime environment is responsible for securely generating and storing these certificates.

A.TargetAdmin

It is assumed that users who are granted administrative privileges to a Target through the TOE are trustworthy and competent to operate that Target.

A.TargetSystem

It is assumed that managed targets are not compromised to the extent that it affects the operation of the agent software of the TOE executing on the managed target.

4 Security Objectives

4.1 Objectives for the TOE

O.UserAuth

The TOE must ensure that only authenticated users can gain access to the TOE and that they must be successfully authenticated before performing any TOE security functions. Additionally, the TOE must mask user passwords during authentication and terminate an interactive session after an administrator-specified period of time.

O.ObjectAccess

The TOE shall enforce an Privilege-Based Access Control policy in order to allow administrators to restrict access to managed objects to authorized users.

O.Auditing

The TOE shall generate audit records for security-relevant actions and make that information available to authorized personnel.

O.SecComs

The TSF must ensure that data transferred between the remote parts of the TOE is protected against disclosure and modification.

O.CompManage

The TOE shall offer a mechanism to detect deviations between configurations of managed targets and administrator-defined baseline configurations and report on any compliance violations.

O.TSFDataCom

The TSF must provide the capability to consistently interpret X.509 certificates (according to specified implementation standards) when shared between the TOE and the trusted underlying operating system of the OMS.

4.2 Objectives for the IT Environment

OE.Auth

The runtime environment for the TOE shall implement authentication mechanisms sought by the TOE and provide authentication decisions for the TOE users to the TSF.

OE.Timestamp

The runtime environments for the OMS shall supply a reliable time source for the TOE's usage.

4.3 Objectives for the Non-IT Environment

OE.Admin

Those responsible for the administration of the TOE are competent and trustworthy individuals who are not careless, willfully negligent, or hostile and also will follow the provided guidance documentation to install, configure, operate, and manage the TOE and its operational environment properly.

OE.Runtime

Those responsible for the administration of the TOE must ensure that the systems hosting parts of the TOE are used solely for this purpose and configured properly (i.e. not running application software except as required) to prevent unauthorized access to the TOE and the security information it contains. This also includes prevention against unauthorized physical access and network-related attacks.

OE.KeyProtect

The runtime environment for the TOE shall securely generate, store, and import X.509 certificates to the TOE for its usage in providing secure communications between the OMS and the agent.

OE.TargetAdmin

Those granted administrative privileges to a Target through the TOE are competent and trustworthy individuals who are not careless, willfully negligent, or hostile with respect to the Target, its agent, or its users.

OE.TargetSystem

Managed target systems have sufficient protection measures and are configured to protect the agent software of the TOE from unauthorized tampering.

4.4 Security Objectives Rationale

4.4.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.UserAuth	T.User T.Inactive T.Mask
O.ObjectAccess	T.Access
O.Auditing	T.Auditing
O.SecComs	T.Compromised
O.CompManage	T.Compliance
O.TSFDataCom	T.TSFDataCom

Table 1: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the IT environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.Auth	T.User
OE.Timestamp	T.Auditing

Table 2: Mapping of security objectives for the IT environment to assumptions, threats and policies

The following table provides a mapping of the objectives for the non-IT environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.Admin	A.InstallConfig A.Admin
OE.Runtime	A.Physical A.SelfProtect
OE.KeyProtect	A.KeyProtect
OE.TargetAdmin	A.TargetAdmin
OE.TargetSystem	A.TargetSystem T.Compliance

Table 3: Mapping of security objectives for the non-IT environment to assumptions, threats and policies

4.4.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.User	The threat that an attacker may gain access to the TOE without being properly authenticated is diminished by O.UserAuth which ensures that only authenticated users can gain access to the TOE and that they must be successfully authenticated before performing any TOE security functions. This is supported by OE.Auth which requires that the operational environment to provide authentication decisions to the TOE in order for the TOE to authenticate users to the TSF.
T.Access	The threat that users can gain access to managed objects stored in the OMS without proper authorization is diminished by O.ObjectAccess which ensures that users are subject to that Privilege-Based Access Control policy when gaining access to the managed objects in the TOE.

Threat	Rationale for security objectives
T.Auditing	The threat that security-relevant activities of unauthorized users may go unnoticed is diminished by O.Auditing which requires the TOE to generate audit records for security-relevant events. This is supported by OE.Timestamp, which requires the operational environment to provide a reliable time source for the time stamps generated as part of the audit record.
T.Compromised	The threat that data may be compromised while transferring between the remote parts of the TOE is diminished by O.SecComs which requires the TOE to provide mechanisms to protect data from disclosure or modification when being transferred between remote entities of the TOE.
T.Compliance	The threat that configurations of the target systems deviated from the administrator-defined policies may be undetected is diminished by O.CompManage which requires to the TOE to offer functionality to compare the configuration of managed targets against administrator-defined policies and notify administrators of compliance violations. In addition, the problem that a compromised target system can not report compliance problems is addressed by OE.TargetSystem requiring sufficient protection of the agent software within the target system.
T.Inactive	The threat that an unauthorized user may gain access to a user session after a period of inactivity to obtain confidential data is diminished by O.UserAuth which requires the TSF to perform user session termination after it becomes inactive for a specified period of time.
T.Mask	The threat that a user may gain unauthorized access by viewing users entering their passwords during the authentication process is diminished by O.UserAuth which requires the TSF to mask passwords during the authentication process.
T.TSFDataCom	The threat that an authorized or unauthorized user may compromise the TSF data (i.e. X.509 certificates used for SSL communications between the OMS and the agents) that are shared between the TOE and the trusted underlying operating system of the OMS is diminished by O.TSFDataCom which requires the TSF to provide the capability to consistently interpret X.509 (according to specified implementation standards) certificates shared between these two entities.

Table 4: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.Physical	The assumption on the physical protection of the TOE and its runtime environment is accomplished by OE.Runtime which requires for the TOE as well as its runtime environment to be physically protected against unauthorized access.
A.Admin	The assumption that the administrators of the TOE and of the operational environment are trustworthy and competent to administer the TOE and its operational environment is achieved by OE.Admin which ensures these properties of administrators.
A.SelfProtect	The assumption that the machines providing the runtime environments for the TOE are used exclusively for this purpose and configured properly (i.e. not running other application software not required) as well as preventing unauthorized access is addressed by OE.Runtime which requires the IT environment to implement respective measures for the runtime environments.
A.KeyProtect	The assumption that X.509 certificates used for securing communications between the OMS and the agent are imported from the TOE's runtime environment and also the runtime environment is responsible for secure generation and storage of these certificates is met by OE.KeyProtect which requires the IT environment to provide those capabilities.
A.TargetAdmin	The assumption that the users who are granted administrative privilege to a Target through the TOE are trustworthy and competent to operate that Target is achieved by OE.TargetAdmin which ensures these properties of target administrators.
A.TargetSystem	The assumption that managed target systems are not compromised is addressed by OE.TargetSystem, which requires the existence and use of security functions of the target system to protect the agent software and data from unauthorized tampering.
A.InstallConfig	The assumption that the TOE is installed, configured, and operated in its evaluated configuration in accordance to the Security Target and the TOE guidance is covered by OE.Admin which ensures that administrators abide by the provided guidance. Additionally, those responsible for the administration of the TOE are competent, trustworthy and not careless, willfully negligent, or hostile.

Table 5: Sufficiency of objectives holding assumptions

5 Extended Components Definition

This ST defines the extended component FDP_SDA.1 as part of a new family FDP_SDA of class FDP in CC Part 2 for usage within this ST.

Family FDP_SDA is defined as follows:

Family behaviour

This family describes the capability to manage security compliance/deviations of the targets that the TOE manages. In other words, the TSF perform comparisons of the configurations of managed targets, i.e. security-relevant configuration settings, against baseline configurations defined by administrator, and reports identified deviations.

Component levelling

This family consists of only one component, i.e. FDP_SDA.1, which covers both the requirement on the TSF to apply rules to detect configuration deviations as well as the requirement on the TSF to notify administrators in case of detected deviations.

5.1 Class FDP:

5.1.1 Sample Deviation Analysis (SDA)

Management: FDP_SDA.1

The following actions could be considered for the management functions in FMT:

a) Specification of baseline configurations for targets.

Audit: FDP_SDA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Creation, modification and deletion of baselines.

b) Minimal: Detection of deviations from the baseline configuration.

5.1.1.1 FDP_SDA.1 - Sample Deviation Analysis

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDA.1.1 The TSF shall be able to apply a set of rules to detect deviations of individual target configurations from administrator-defined baseline configurations.

FDP_SDA.1.2 The TSF shall provide a means to notify administrators about detected deviations.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the Security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional class	Security functional requirement	Security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review		CC Part 2	No	No	Yes	No
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation		CC Part 2	No	No	Yes	No
	FCS_COP.1a Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1b Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1d Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1f Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
FDP - User data protection	FDP_ACC.1a Subset access control	FDP_ACC.1	CC Part 2	Yes	No	Yes	No
	FDP_ACC.1b Subset access control	FDP_ACC.1	CC Part 2	Yes	No	Yes	No
	FDP_ACF.1a Security attribute based access control	FDP_ACF.1	CC Part 2	Yes	No	Yes	No
	FDP_ACF.1b Security attribute based access control	FDP_ACF.1	CC Part 2	Yes	No	Yes	No
	FDP_ITT.1 Basic internal transfer protection		CC Part 2	No	No	Yes	Yes
FDP - User data protection	FDP_SDA.1 Sample deviation analysis		ECD	No	No	No	No
FIA - Identification and authentication	FIA_ATD.1 User attribute definition		CC Part 2	No	No	Yes	No

Security functional class	Security functional requirement	Security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FIA_UAU.1 Timing of authentica tion		CC Part 2	No	No	Yes	No
	FIA_UAU.2 User authentication before any action		CC Part 2	No	No	No	No
	FIA_UAU.7 Protected authenti cation feedback		CC Part 2	No	No	Yes	No
	FIA_UID.1 Timing of identifica tion		CC Part 2	No	No	Yes	No
	FIA_UID.2 User identification before any action		CC Part 2	No	No	No	No
	FIA_USB.1 User-subject binding		CC Part 2	No	No	Yes	No
FMT - Security management	FMT_MSA.1a Management of security attributes	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1b Management of security attributes	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.3 Static attribute ini tialisation		CC Part 2	No	No	Yes	Yes
	FMT_MTD.1 Management of TSF data		CC Part 2	No	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles		CC Part 2	No	No	Yes	No
FPT - Protection of the TSF	FPT_TDC.1 Inter-TSF basic TSF data consistency		CC Part 2	No	Yes	Yes	No
	FPT_ITT.1 Basic internal TSF data transfer protection		CC Part 2	No	No	No	Yes
FTA - TOE access	FTA_SSL.3 TSF-initiated termi nation		CC Part 2	No	Yes	Yes	No

Table 6: Security functional requirements for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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)
- **logon/logoff**
- **user management (creation, deletion, modification)**
- **user password change**
- **role management**
- **privilege management**
- **job management (submission, edit, deletion)**
- **file transfer**
- **remote operations (i.e. alerts sent back from the agents about job status)**

.

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,

- **the name and IP address of the user's host machine**

.

6.1.1.2 User identity association (FAU_GEN.2)

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.

6.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **authenticated users** with the capability to read **all audit information** from the audit records.

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

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **SSLv3 symmetric key and secret generation** and specified cryptographic key sizes **168 Bits (3-DES keys) and 160 Bits (HMAC SHA-1 secret)** that meet the following:

1. **[SSLv3] (SSLv3 symmetric key and secret generation),**
2. **[SP800-67] (3-DES key generation)**

.

6.1.2.2 Cryptographic operation (FCS_COP.1a)

FCS_COP.1.1 The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm

1. **3-DES (CBC mode)**

and cryptographic key sizes

1. **168 Bits (3-DES)**

that meet the following:

1. **[FIPS46-3], [FIPS81] (3-DES, CBC mode)**

.

6.1.2.3 Cryptographic operation (FCS_COP.1b)

FCS_COP.1.1 The TSF shall perform **key wrapping** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, or 2048 bits** that meet the following: **[RFC2313] (RFC 2313), [RFC2437](RFC 2437), and [SSLv3] (The SSL Protocol, Version 3)**.

6.1.2.4 Cryptographic operation (FCS_COP.1d)

FCS_COP.1.1 The TSF shall perform **RSA signature generation/verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, or 2048 bits** that meet the following: **[PKCS1] (PCKS#1), [SSLv3] (The SSL Protocol, Version 3)**.

6.1.2.5 Cryptographic operation (FCS_COP.1f)

FCS_COP.1.1 The TSF shall perform **data authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA-1** and cryptographic key sizes **160 bits** that meet the following: **[FIPS180] (FIPS 180), [FIPS198] (FIPS 198), [SSLv3] (SSLv3)**.

6.1.3 User data protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1a)

FDP_ACC.1.1 The TSF shall enforce the **Privilege-Based Access Control SFP** on

- **processes representing authorized users as subjects**
- **objects stored in the Oracle Management Repository**
- **all operator requests, i.e. all operations requested by the subjects on these objects, that require operator or full privileges**

.

6.1.3.2 Subset access control (FDP_ACC.1b)

FDP_ACC.1.1 The TSF shall enforce the **Protected Data Transfer SFP** on

- **agents and OMS host as subjects**
- **target information collected by the TOE as objects**

- **the transfer of objects across the network as operations**

.

6.1.3.3 Security attribute based access control (FDP_ACF.1a)

FDP_ACF.1.1 The TSF shall enforce the **Privilege-Based Access Control SFP** to objects based on the following:

- **subject security attributes:**
  - **user ID**
  - **privileges granted to a user**
  - **roles assigned to a user**
- **object security attributes:**
  - **in case of targets:**
    - **target ID**
    - **group membership**
      - **privilege propagation groups assigned to group**
  - **in case of other objects:**
    - **object identifier**

.

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

- **A request to perform normal administrative operations on the target object, such as configure a blackout or edit the properties of a target is granted if the subject, or a role that has been assigned to the subject, has been assigned the OPERATOR_TARGET privilege for the requested object (or for a group that the target is a member of).**
- **A request to perform any operations on the target, including delete a target is granted if the subject, or a role that has been assigned to the subject, has been assigned the FULL_TARGET privilege for the requested object (or for a group that the target is a member of).**
- **A request to view target information, is granted if the subject, has been assigned VIEW_ANY_TARGET privilege for the requested object (or for a group that the target is a member of).**
- **A request to view properties, inventory and monitor information about a target is granted if the subject, or a role that has been assigned to the subject, has been assigned the VIEW_TARGET privilege for the requested object (or for a group that the target is a member of).**

- **A request to create, edit, schedule, or stop a blackout on the target object is granted if the subject, or a role that has been granted to the subject, has been assigned the BLACKOUT_TARGET privilege for the requested object (or for a group that the target is a member of).**
- **A request to clear stateless alerts, manually re-evaluate alerts, or acknowledge alerts for target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the MANAGE_TARGET_ALERTS privilege for the requested object (or for a group that the target is a member of).**
- **A request to edit threshold or metric and policy setting, applying monitoring templates, or manage User Defined Metrics of target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the MANAGE_TARGET_METRICS privilege for the requested object (or for a group that the target is a member of).**
- **A request to delete a target, or configure credentials for its maintenance, is granted if the subject, or a role that has been assigned to the subject, has been assigned the CONFIGURE_TARGET privilege for the requested object (or for a group that the target is a member of).**
- **A request to add a target is granted if the subject, or a role that has been assigned to the subject, has been assigned the CREATE_TARGET privilege for the requested object (or for a group that the target is a member of).**
- **A request to create privilege propagating group targets is granted if the subject, or a role that has been assigned to the subject, has been assigned the CREATE_PROPAGATING_GROUP privilege for the requested object (or for a group that the target is a member of).**
- **A request to administer group targets is granted if the subject, or a role that has been assigned to the subject, has been assigned the GROUP_ADMINISTRATION privilege for the requested object (or for a group that the target is a member of).**
- **A request to view and do a create-like (clone) on a job on a target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the VIEW_JOB privilege for the requested object (or for a group that the target is a member of).**
- **A request to submit, modify, do a create-like (clone), delete a job on a target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the FULL_JOB privilege for the requested object (or for a group that the target is a member of).**
- **A request to publish reports for public viewing on a target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the PUBLISH_REPORT privilege for the requested object (or for a group that the target is a member of).**

- **A request to view report definition and stored reports, generate on demand reports, or do a create-like (clone) on a target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the VIEW_REPORT privilege for the requested object (or for a group that the target is a member of).**
- **A request to view a template on a target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the VIEW_TEMPLATE privilege for the requested object (or for a group that the target is a member of).**
- **A request to apply, modify, delete a template on a target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the FULL_TEMPLATE privilege for the requested object (or for a group that the target is a member of).**
- **A request to read related actions on target properties, inventory, monitoring information on target object is granted if the subject, or a role that has been assigned to the subject, has been assigned the EM_MONITOR privilege for the requested object (or for a group that the target is a member of).**
- **The assignment/revocation of roles to a user ID is granted if the subject has been assigned the SUPER USER role, or has the SYSMAN user ID.**
- **The assignment/revocation of a privilege to a user ID is granted if the subject has been assigned the SUPER USER role, has the SYSMAN user ID, or is the owner of the object.**
- **The modification of OMS host certificate is granted if the subject has been assigned the SUPER USER role.**

Application Note: Within the ST and scope of evaluation, the term group has a distinct meaning, and it does not refer to all kinds of aggregated targets.

.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **following additional rules: none**.

6.1.3.4 Security attribute based access control (FDP_ACF.1b)

FDP_ACF.1.1 The TSF shall enforce the **Protected Data Transfer SFP** to objects based on the following:

- **subjects and objects as defined in FDP_ACC.1b**
- **subject security attributes: OMS host certificate**
- **object security attributes: none**

.

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

- **If a protected network connection is established using the OMS host certificate, then all transfers are allowed; otherwise, transfers are denied**

.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **following additional rules: none**.

6.1.3.5 Basic internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1 The TSF shall enforce the **Protected Data Transfer SFP** to prevent the **disclosure, modification** of user data when it is transmitted between physically-separated parts of the TOE.

6.1.4 User data protection (FDP)

6.1.4.1 Sample deviation analysis (FDP_SDA.1)

FDP_SDA.1.1 The TSF shall be able to apply a set of rules to detect deviations of individual target configurations from administrator-defined baseline configurations.

FDP_SDA.1.2 The TSF shall provide a means to notify administrators about detected deviations.

6.1.5 Identification and authentication (FIA)

6.1.5.1 User attribute definition (FIA_ATD.1)

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

- **user of GUI/CLI**
  - **user ID**
  - **roles assigned to the user**
  - **privileges granted to the user**
- **agent**
  - **identifier**
  - **agent password**
- **OMS**
  - **X.509 certificates**

.

6.1.5.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **access to the online help** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: This is for user/management interfaces (i.e. OMS-provided CLI and GUI). Here, the TOE only enforces authentication decisions provided to it by the operational environment (i.e. Database Repository).

6.1.5.3 User authentication before any action (FIA_UAU.2)

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

Application Note: This applies to the authentication between the OMS and agent.

6.1.5.4 Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **masked characters** to the user while the authentication is in progress.

6.1.5.5 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow **access to the online help** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: This SFR applies to the identification of users via the CLI/GUI interface.

6.1.5.6 User identification before any action (FIA_UID.2)

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

Application Note: This applies to the authentication between the OMS and agent.

6.1.5.7 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **user of GUI/CLI**
  - **user ID**
  - **roles assigned to the user**
  - **privileges granted to the user**
- **agent**
  - **identifier**
  - **agent password**
- **OMS**
  - **X.509 certificates**

.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **none**.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **changes shall be effective immediately**.

6.1.6 Security management (FMT)

6.1.6.1 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1.1 The TSF shall enforce the **Privilege-Based Access Control SFP** to restrict the ability to **query, modify, delete** the security attributes **role assignment, privilege assignment, group membership, and privilege propagation group membership** to **the SUPER USER role**.

6.1.6.2 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1.1 The TSF shall enforce the **Privilege-Based Access Control SFP** to restrict the ability to **modify** the security attributes **OMS host certificate** to **the SUPER USER role**.

6.1.6.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Privilege-Based Access Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **SUPER USER role** to specify alternative initial values to override the default values when an object or information is created.

6.1.6.4 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to **query, modify, delete** the

- **definition of target configuration baselines**

to **administrator-defined roles that contain OPERATOR_TARGET privilege**.

6.1.6.5 Specification of management functions (FMT_SMF.1)

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

- **user, privilege and role management**
- **audit management**
- **baseline configuration management**
- **credential management of target (e.g., setting preferred credentials)**
- **certificate management**
- **compliance notification management**

.

6.1.6.6 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

- **SUPER USER**
- **other administrator-defined roles**

.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.7 Protection of the TSF (FPT)

6.1.7.1 Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret

- **public key certificates**
- **private keys**

when shared between the TSF and *the underlying operating system of the OMS as a trusted IT product.*

FPT_TDC.1.2 The TSF shall use **PKCS#12 [PKCS12]** when interpreting the TSF data from *the underlying operating system of the OMS as a trusted IT product.*

6.1.7.2 Basic internal TSF data transfer protection (FPT_ITT.1)

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

6.1.8 TOE access (FTA)

6.1.8.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after *an***administrator-defined time interval of user inactivity**.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security Functional Requirements	Objectives
FAU_GEN.1	O.Auditing
FAU_GEN.2	O.Auditing
FAU_SAR.1	O.Auditing
FCS_CKM.1	O.SecComs, O.TSFDataCom

Security Functional Requirements	**Objectives**
FCS_COP.1a	O.SecComs, O.TSFDataCom
FCS_COP.1b	O.SecComs, O.TSFDataCom
FCS_COP.1d	O.SecComs, O.TSFDataCom
FCS_COP.1f	O.SecComs, O.TSFDataCom
FDP_ACC.1a	O.ObjectAccess
FDP_ACC.1b	O.SecComs
FDP_ACF.1a	O.ObjectAccess
FDP_ACF.1b	O.SecComs
FDP_ITT.1	O.SecComs
FDP_SDA.1	O.CompManage
FIA_ATD.1	O.UserAuth
FIA_UAU.1	O.UserAuth
FIA_UAU.2	O.UserAuth
FIA_UAU.7	O.UserAuth
FIA_UID.1	O.UserAuth
FIA_UID.2	O.UserAuth
FIA_USB.1	O.UserAuth
FMT_MSA.1a	O.ObjectAccess
FMT_MSA.1b	O.SecComs
FMT_MSA.3	O.ObjectAccess, O.SecComs
FMT_MTD.1	O.CompManage
FMT_SMF.1	O.Auditing, O.CompManage, O.ObjectAccess, O.SecComs, O.UserAuth

Security Functional Requirements	Objectives
FMT_SMR.1	O.Auditing, O.CompManage, O.ObjectAccess, O.SecComs, O.UserAuth
FPT_TDC.1	O.TSFDataCom
FPT_ITT.1	O.SecComs
FTA_SSL.3	O.UserAuth

Table 7: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.UserAuth	The objective to allow only authorized users access to the TOE is met by FIA_UAU.1, FIA_UAU.2, FIA_UID.1, and FIA_UID.2. The TOE is able to maintain and associate security attributes belonging to respective users (FIA_ATD.1, FIA_USB.1). Authentication data is protected by masking characters (FIA_UAU.7). An interactive session will be terminated after a period of inactivity as specified in FTA_SSL.3. It is supported by requirements pertaining to the management of the access control enforcement (FMT_SMF.1, FMT_SMR.1).
O.ObjectAccess	The objective to allow the restriction of access to managed objects is implemented by a Privilege-Based Access Control policy as specified in FDP_ACC.1a and FDP_ACF.1a. It is supported by requirements pertaining to the management of the access control enforcement (FMT_MSA.1a, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1).
O.Auditing	The objective to provide means to audit changes to security-relevant events is addressed by requirement for the generation of audit records (FAU_GEN.1, FAU_GEN.2). Administrators have the ability to review audit data (FAU_SAR.1). Supportive management functionality is defined in FMT_SMF.1, and FMT_SMR.1.
O.SecComs	FPT_ITT.1 defines the requirement to protect TSF data that is being transferred between the TOE parts. FDP_ACC.1b, FDP_ACF.1b, and FDP_ITT.1 define the requirement to protect user data that is being transferred between the TOE parts. FMT_MSA.1b and FMT_MSA.3 define

Security objectives	Rationale
	the requirement to manage the certificates used by SSL in protecting the user data. The cryptographic mechanisms used to implement SSL communication channels are spelled out in FCS_CKM.1, FCS_COP.1a, FCS_COP.1b, FCS_COP.1d, and FCS_COP.1f.
O.CompManage	The objective to provide means to apply a set of rules to detect deviations of target configurations from administrator-defined baseline configurations is met by FDP_SDA.1. Supportive management functionality is spelled out in FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.
O.TSFDataCom	FPT_TDC.1 defines the requirement to protect TSF data that is being transferred between the TOE and another trusted IT product. The cryptographic mechanisms used to implement SSL communication channels are spelled out in FCS_CKM.1, FCS_COP.1a, FCS_COP.1b, FCS_COP.1d, and FCS_COP.1f.

Table 8: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	This dependency is not resolved. Unresolved dependency rationale: the TOE assumes that the runtime environment provides a reliable time source for the generation of audit records.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1a FCS_COP.1f
	FCS_CKM.4	This dependency is not resolved. Unresolved dependency rationale: Keys used for authentication (i.e. SSL sessions) are not formally destroyed - object reuse mechanisms in the runtime environment prevent their use except for in the intended context.

Security Functional Requirement	Dependencies	Resolution
FCS_COP.1a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is not resolved. Unresolved dependency rationale: Keys are not formally destroyed - object reuse mechanisms in the runtime environment prevent their use except for in the intended context.
FCS_COP.1b	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is not resolved. Unresolved dependency rationale: FCS_CKM.1 is not applicable because the TOE does not generate these keys by itself. FPT_TDC.1 has been explicitly selected to model the transfer of keys (to be used for key wrapping) from the trusted underlying operating system of the OMS into the TSF.
	FCS_CKM.4	This dependency is not resolved. Unresolved dependency rationale: RSA keys lifetimes are indefinitely long and therefore destruction is not applicable. The keys are stored by the operating system and are protected explicitly by A.KeyProtect.
FCS_COP.1d	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is not resolved. Unresolved dependency rationale: FCS_CKM.1 is not applicable because the TOE does not generate RSA keys by itself. FPT_TDC.1 has been explicitly selected to model the transfer of keys (to be used for key wrapping) from the trusted underlying operating system of the OMS into the TSF.
	FCS_CKM.4	This dependency is not resolved. Unresolved dependency rationale: RSA keys lifetimes are indefinitely long and therefore destruction is not applicable. The keys are stored by the operating system and are protected explicitly by A.KeyProtect.

Security Functional Requirement	**Dependencies**	**Resolution**
FCS_COP.1f	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is not resolved. Unresolved dependency rationale: cryptographic secrets are not formally destroyed - object reuse mechanisms in the runtime environment prevent their use except for in the intended context.
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b
FDP_ACF.1a	FDP_ACC.1	FDP_ACC.1a
	FMT_MSA.3	FMT_MSA.3
FDP_ACF.1b	FDP_ACC.1	FDP_ACC.1b
	FMT_MSA.3	FMT_MSA.3
FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1b
FDP_SDA.1	No dependencies.	
FIA_ATD.1	No dependencies.	
FIA_UAU.1	FIA_UID.1	FIA_UID.1 Note that both FIA_UAU.1 and FIA_UID.1 apply to the identification and notification of users only.
FIA_UAU.2	FIA_UID.1	FIA_UID.2 Note that both FIA_UAU.2 and FIA_UID.1 apply to the identification and notification of agents only.
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies.	
FIA_UID.2	No dependencies.	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1a	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1a
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1

Security Functional Requirement	**Dependencies**	**Resolution**
FMT_MSA.1b	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1b
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1a FMT_MSA.1b
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies.	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_TDC.1	No dependencies.	
FPT_ITT.1	No dependencies.	
FTA_SSL.3	No dependencies.	

Table 9: TOE SFR dependency analysis

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components, augmented by ALC_FLR.3, as specified in [CC] part 3. No operations are applied to the assurance components.

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE. In addition, the evaluation assurance level has been augmented with ALC_FLR.3 to be commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

7 TOE Summary Specification

7.1 TOE Security Functionality

The following section explains how the security functions are implemented. The different TOE security functions cover the various SFR classes.

The primary security features of the TOE are:

- Identification and Authentication
- Privilege-Based Access Control
- Auditing
- Protected Data Transfer
- Compliance Management
- Security Management

7.1.1 Identification and authentication

The TOE enforces authentication decisions made by the OM repository in the IT environment on users accessing the TOE via the OMS-provided GUI or CLI interface (FIA_UAU.1). It receives user credentials (e.g., user ID, passwords) from the requesting user, passes these on to the repository (database) and accepts/rejects users based on the decision provided by the database. It then uses the user name provided in successful authentication requests to identify users (FIA_UID.1). The TOE allows users to access online help through the GUI and CLI interfaces prior to performing identification and authentication.

In addition, the TOE maintains security attributes (ID, role, privileges) of its users (FIA_ATD.1) and associates these attributes with subjects acting on behalf of those users (FIA_USB.1). The TOE also provides protected authentication feedback while user authentication is in progress (FIA_UAU.7).

Additional forms of authentication performed by the TOE involve the use of SSL certificates, agent registration passwords, and agent keys which are explained as follows:

- Agent registration passwords are passwords that act as the "bootstrap" trust between the agents and OMS. These passwords are defined by administrators and provided by agents for use during installation. When a new agent registers with the OMS, the OMS will verify whether the agent possesses this password by performing a challenge-response protocol. Upon successful validation of the agent registration password, the agent and OMS generate agent keys based on the random numbers exchanged previously between them and the agent registration password. The agent keys are then negotiated where both entities verify that the HTTPS headers exchanged between them contain this password (FIA_UAU.2, FIA_UID.2, FCS_COP.1a). Upon successful verification, the OMS generates the server certificate along with associated CA's and trusted certificates for the agent to download. The agent then uses that certificate to establish secure communications with OMS.
- Afterwards, when a connection is made between the agent and another entity (i.e. OMS), that entity may authenticate itself by participating in a challenge response with the agent. This verifies to the agent that the entity's private key corresponds to the public key in the OMS certificate that was given to the agent previously.''

These additional forms of authentication require successful identification and authentication of an agent or OMS before allowing any other TSF-mediated actions on behalf of that agent or OMS.

In addition, the TOE performs termination of an interactive session after a period of user inactivity defined by the administrator (FTA_SSL.3).

7.1.2 Privilege-based access control

The TOE enforces privilege-based access control policy for administrators using the TOE interfaces to manage targets (FDP_ACC.1a, FDP_ACF.1a) .

Users that are subject to this access control mechanisms are those accessing the TOE via the OMS-provided GUI or CLI interfaces.

Users are granted with certain privileges and roles. Roles allow users to group privileges, and to grant these to users or other roles. In addition, roles can be nested with other roles.

Privileges give the user rights to perform certain management actions within EMGC while roles can be used to limit target access and access to specific management features.

Together privileges and roles control the targets a user can manage and the specific types of tasks the user can perform.

Targets can be grouped into logical sets called target groups. This enables a large number of targets to be organized, managed, and effectively monitored. Groups can include targets of the same type (e.g., all hosts in the organization's data center or all of the production databases), or targets of different types (e.g., the database, operating system within a particular data center region).

Privileges can be associated with either individual target or a group. The following privileges are supported:

- SYSTEM privileges
  - SUPER_USER: provides all privileges and full access to all targets as well as enables privilege and role management capabilities and modification of OMS host certificate
- TARGET privileges
  - CREATE_TARGET: ability to create a target
  - VIEW_ANY_TARGET: ability to view properties, inventory, monitoring information about any target
  - CREATE_PROPAGATING_GROUP: ability to create a propagating group.
  - VIEW_TARGET: ability to view properties, inventory, and monitor information about a target
  - BLACKOUT_TARGET: ability to create, edit, schedule, or stop a blackout on a target
  - MANAGE_TARGET_METRICS: ability to edit threshold, metric or policy settings, apply monitoring templates, manage user defined metrics
  - CONFIGURE_TARGET: ability to delete target, configure target credentials
  - MANAGE_TARGET_ALERTS: ability to clear stateless alerts, manually re-evaluate alerts or acknowledge alerts for a target properties
  - OPERATOR_TARGET: ability to perform actions related to BLACKOUT_TARGET, MANAGE_TARGET_METRICS, CONFIGURE_TARGET, MANAGE_TARGET_ALERTS
  - FULL_TARGET: ability to manage all actions on privileges as well as actions on OPERATOR_TARGET
  - GROUP_ADMINISTRATION: ability to administer group targets such as add/delete membership, modify user privileges of targets in a group, and if group is privilege propagating, then also all actions of FULL_TARGET

    - EM_MONITOR: ability to read related actions on target properties, inventory, and monitoring information

- JOB privileges
    - VIEW_JOB: ability to view, or do a create-like (clone) job
    - FULL_JOB: ability to submit, modify, create-like (clone), delete jobs
- REPORT privileges
    - PUBLISH_REPORT: ability to publish reports for public viewing
    - VIEW_REPORT: ability to view report definition and stored reports, generate on demand reports or do a create-like (clone)
- TEMPLATE privileges
    - VIEW_TEMPLATE: ability to view a template
    - FULL_TEMPLATE: ability to apply templates to a target, modify or delete templates

There are two types of user accounts in the TOE: super administrator and administrator.

The super administrator account is called SYSMAN which is a default account created during installation of the EMGC. In particular, a super administrator is assigned the SUPER USER role. This account can neither be deleted nor the privileges associated to it can be revoked. Additionally, this account has unrestricted access including the ability to manage all other administrator accounts and set up all administrator credentials, create privileges and roles, and perform any action on any target in the system. In addition, a super administrator can access any object and control its security attributes, including objects owned by other administrators.

Administrator accounts, on the other hand, provide users permission to perform administrative tasks and access administrative information. Users with this type of account can have access to a subset of operations and will only see or be able to modify those jobs, events, or groups to which they have been granted access by the super administrator or other administrators.

7.1.3 Auditing

The TSF implements generation of audit records (FAU_GEN.1) of security-relevant activities stimulated by its users. Auditing is provided mainly by the PL/SQL part of the TOE which covers the following types of events:

- authentication attempts
- logon/logoff
- user management
- security attribute management
- job management
- file transfer
- remote operations

Audit records contain the following information:

- type of event
- date and time of the event
- user identity (if applicable)
- outcome of the event (success/failure)
- name and IP address of the user's host system

For each audit auditable event, the TOE associates the event with the identity of the user that caused the event (FAU_GEN.2).

In addition, the TOE offers the capability to review audit events to authenticated users (FAU_SAR.1).

7.1.4 Protected data transfer

The TOE implements SSL to secure communication between the OMS host and agents against eavesdropping and unauthorized modification of TSF data (FPT_ITT.1) and user data (FDP_ITT.1). The OMS host certificate is used in establishing this connection (FDP_ACC.1b, FDP_ACF.1b). Only FIPS-compliant cipher suites are used in the evaluation configuration:

- 3-DES CBC-based:
    - SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
-

The relevant SFRs are FCS_CKM.1 for generation of SSL symmetric keys and secrets (i.e., session keys generated by the TOE), FCS_COP.1a for encryption and decryption of transferred data in sessions, FCS_COP.1b for RSA key wrapping, FCS_COP.1d for generating and verifying RSA signature, and FCS_COP.1f for HMAC-SHA-1 data authentication.

When an new agent wants to communicate securely with the OMS, it first has to register itself through the use of the agent registration password as described in section "Identification and Authentication" above. Upon successful registration, the OMS's underlying OS generates the server certificate along with associated CA's and trusted certificates for the agent to download. The agent then uses that certificate to establish secure communications with OMS.

For a recurring agent wanting to connect to OMS securely, the agent will renegotiate the agent key and download the new wallet (created by OMS) that contains the credentials of the agent's identity.

Cryptographic keys (i.e. X.509 certificates) used by the OMS and the agents to establish secure communication channels are generated by the underlying OS of the OMS. These certificates are then imported to the OMS from the OMS's operating system. The TOE provides the capability to consistently interpret (according to specified implementation rules) when these certificates are shared between the TOE and the trusted underlying OS of the OMS (FPT_TDC.1).

7.1.5 Compliance management

The TOE performs comparison between configurations of managed targets and configurations defined by administrators (baseline configurations/policies) Additionally, the TOE can generate reports on and notify administrators of any violations of compliance (FDP_SDA.1) resulting from the performed comparison. Examples of violations include inappropriate settings and incorrect system configurations.

Policies defined by administrators contain optimal configurations of systems which are rules against which managed systems are evaluated.

Administrators can also configure the existing policy rule settings, enable, or disable a policy evaluation, or assign a correct action.

Moreover, same configurations/policies can be applied consistently across multiple managed targets by setting up and applying a monitoring template.

Violation alerts generated and sent to administrators contain identification of all the policies, violations as well as compliance scores of the target. Compliance score indicates the percentage to which a target has been compliant with the goals defined by management policies. Compliance score also summarizes all existing defined policies into a useful metric that can be monitored showing the level of compliance of a target. Additionally, compliance score is a combination of severity, importance, and the percentage of objects found to be non-compliant.

Severity refers to the seriousness of the violation and is consisted of several levels. A "Critical" severity denotes a violation that needs immediate attention while a "Warning" warns of serious consequences if the violation is not dealt with in a timely manner. An "Informational" severity imparts knowledge about an object that is violating best practices.

The importance level denotes the impact of the policy violation against this target.. A "High" importance level indicates that the system could be compromised if a security policy rule violation is ignored.

7.1.6 Security management

The TOE offers administrative interfaces such as OMS-provided GUI and CLI (FMT_SMF.1) to manage the TOE security functions as follows:

- Management of security attributes used for the enforcement of the Privilege-Based Access Control policy (FMT_MSA.1a, FMT_MSA.3)
- Management of TSF data including restricting the ability to query, modify, delete definition of target configuration baselines to authorized administrators (FMT_MTD.1)
- Management functions including audit management, security attribute management, baseline configuration management, and credential management of target objects (FMT_SMF.1)
- Management of SSL certificates (FMT_MSA.1b, FMT_MSA.3)
- Management of security roles as defined in FMT_SMR.1.

The CLI, text-based consoles (e.g., shell and command windows), allows administrators to perform same operations as the OMS-provided GUI such as monitoring/management targets, jobs, groups, blackouts, notifications, and alerts. The CLI interface is fully integrated with EMGC's security and user administration functions, thus allowing administrators to carry out operations with the same security as the GUI interface.

8 Abbreviations, Terminology and References

8.1 Abbreviations

CLI

Command Line Interface

EMGC

Enterprise Manager Grid Control

GUI

Graphical User Interface

HTTPS

Hypertext Transfer Protocol over Secure Socket Layers

OMS

Oracle Management Server

PL-SQL

Procedural Language/Structured Query Language

SDK

Software Development Kit

SSL

Secure Sockets Layer

VPD

Virtual Private Database

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator

The term administrators is used through this ST occasionally to refer to user who are authorized (by privilege or role assignment) to perform administrative actions.

Authorized users

Any user who is granted with specified privileges and/or roles.

operator request

Any request that requires operator or full privileges for the target. Operator privileges allow startup or shutdown of the target, or editing target properties. Full privileges, in addition, allow deletion of targets and the configuration of target credentials.

Subject

A subject is a process representing a user and other entities of the TOE acting on behalf of users.

8.3 References

CAPP **Common Criteria Protection Profile, Version 1.d, 8 October 1999, Information Assurance Directorate, National Security Agency.**
Version 1.d
Date September 8, 1999

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R3
Date July 2009
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf

CEM **Common Methodology for Information Technology Security Evaluation**
Version 3.1R3
Date July 2009
Location http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf

FIPS180 **Secure Hash Standard**
Date May 11, 1993

FIPS198 **The Keyed-Hash Message Authentication Code (HMAC)**
Date March 6, 2002
Location http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

FIPS46-3 **FIPS PUB 46-3: DATA ENCRYPTION STANDARD (DES).**
Date October 25, 1999

FIPS81 **FIPS PUB 81: DES Modes of Operations.**
Date December 2, 1980

PKCS1 **RFC 2313: PKCS #1: RSA Encryption Version 1.5**
Date March 1998
Location http://www.faqs.org/rfcs/rfc2313.html

PKCS12 **PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories**
Date June 24, 1999

RFC2313 **RFC 2313: PKCS#1: RSA Cryptography Specification, Version 1.5.**
Date March 1998

RFC2437 **RFC 2437: PKCS #1: RSA Cryptography Specifications, Version 2.0.**
Date October 1998

SP800-67 **NIST Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher**
Date May 19, 2008
Location http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

SSLv3 **Alan O. Freier, Philip Karlton, Paul C. Kocher: The SSL Protocol, Version 3.**
Date November 1996
Location http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt