Mobiledesk VPN v1.0
Security Target v1.3

SAMSUNG SDS

Revision History

No.	Version	Reason for Revision	Revision Date
1	1.0	1st draft	2010.12.28
2	1.1	Added Operational environment structure	2011.05.26
3	1.2	Added Operating System	2011.06.15
4	1.3	Added Operational environment	2011.07.05

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Table of Contents

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

List of Figures

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

List of Tables

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

1. Security Target Introduction

1.1 Security Target Reference

This section provides information for uniquely identifying the Security Target.

Security Target Title	Mobiledesk VPN v1.0 Security Target
Version	v1.3
Author	Samsung SDS Co., Ltd.
ST Publication Date	July 05, 2011

[Table 1] ST Reference

1.2 TOE Reference

This section provides information for uniquely identifying the TOE.

TOE	Mobiledesk VPN v1.0
TOE Components Build Version	Mobiledesk VPN Client for Android v1.0.4 Mobiledesk VPN Client Library for Android v1.0.4 Mobiledesk VPN Client Library for iOS v1.0.4 Mobiledesk VPN Agent for Linux v1.0.5 Mobiledesk VPN Agent for Windows v1.0.5 Mobiledesk VPN Server v1.0.5 Mobiledesk VPN SPS v1.0.5
Developer	Samsung SDS Co., Ltd.

[Table 2] TOE Reference

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the Mobiledesk VPN v1.0 (hereafter, denoted as "TOE") which provides the Mobile-Based Virtual Private Network (VPN). The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.3.1 Usage and Major Security Features of the TOE

A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides security applying cryptography so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network. The TOE provides VPN functions in mobile wireless network environments such as 3G and WI-FI.

■ Components of the TOE

The Mobiledesk VPN v1.0 is composed of MD_Client, MD_Agent, MD_Server, and MD_SPS.

- **MD_Client**

  The MD_Client is provided as an application or a library. In the ST, the MD_Client refers to the 'MD_Client application' unless it is denoted as 'library'.

  - MD_Client application (Mobiledesk VPN Client for Android v1.0.4)

  The MD_Client can be provided as a VPN client application which is installed and

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

operated on the mobile device using the Android operating system carried by the client user. The client user can perform the Mobile Device Registration after successful authentication, and the mobile device information is transferred to the MD_SPS during registration. After successful registration, the client user can use the Mobile-Based VPN through the 2nd and the 3rd tunneling connections when the MD_Server (the relaying server) exists in the operational environment, or the 3rd tunneling connection only when MD_Server doesn't exist in the operational environment (See [Table 4] and [Table 5] for more details about types of the tunneling provided by the TOE).

- **MD_Client library (Mobiledesk VPN Client Library for Android v1.0.4, Mobiledesk VPN Client Library for iOS v1.0.4)**

The organization which purchases the TOE can use the MD_Client application as VPN client or develop its own VPN client using the MD_Client library for the mobile device based upon Android or iOS operating systems. Therefore, the MD_Client library is composed of management features and cryptography libraries needed for a VPN client, and used by the Client Developer instead of the client user.

• **MD_Agent (Mobiledesk VPN Agent for Linux v1.0.5, Mobiledesk VPN Agent for Windows v1.0.5)**

The MD_Agent, which is installed and operated in a physically secure place in the organization, plays a role of a VPN gateway server which ultimately establishes VPN communication with the MD_Client through the 3rd tunneling connection. In the operational environment with the MD_Server which relays VPN communication, the

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

MD_Agent establishes the 3rd tunneling connection with the MD_Client after successful establishment of the 1st tunneling connection with the MD_Server. The MD_Agent checks if the MD_Client is registered or not for VPN communication, the MD_Agent administrator manages information related to the MD_Client, the client user, and the MD_Server which can communicate with the MD_Agent.

• MD_Server (Mobiledesk VPN Server v1.0.5)

The MD_Server, which is installed and operated in a physically secure place in the organization, plays a role of a VPN gateway server which relays VPN tunneling between the MD_Client and the MD_Agent. The MD_Server checks if the MD_Client and the MD_Agent are registered or not for VPN communication, and relays VPN communication (using remote port forwarding technique) between the MD_Client and the MD_Agent using the 3rd tunneling after successful establishment of the 1st tunneling with the MD_Agent and the 2nd tunneling with the MD_Client.

• MD_SPS (Mobiledesk VPN SPS v1.0.5)

The MD_SPS, which is installed and operated together with the MD_Server in a physically secure place in the organization, plays a role of a management server for the MD_Server and trusted authentication server for server authentication. The MD_Server administrator can review the audit data generated by both the MD_Server and the MD_SPS, set configurations, and start/stop the MD_Server and the MD_SPS through the MD_SPS. Also, the MD_Server administrator manages information related to the MD_Agent and the mobile device for the MD_Client which can communicate with the MD_Server.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

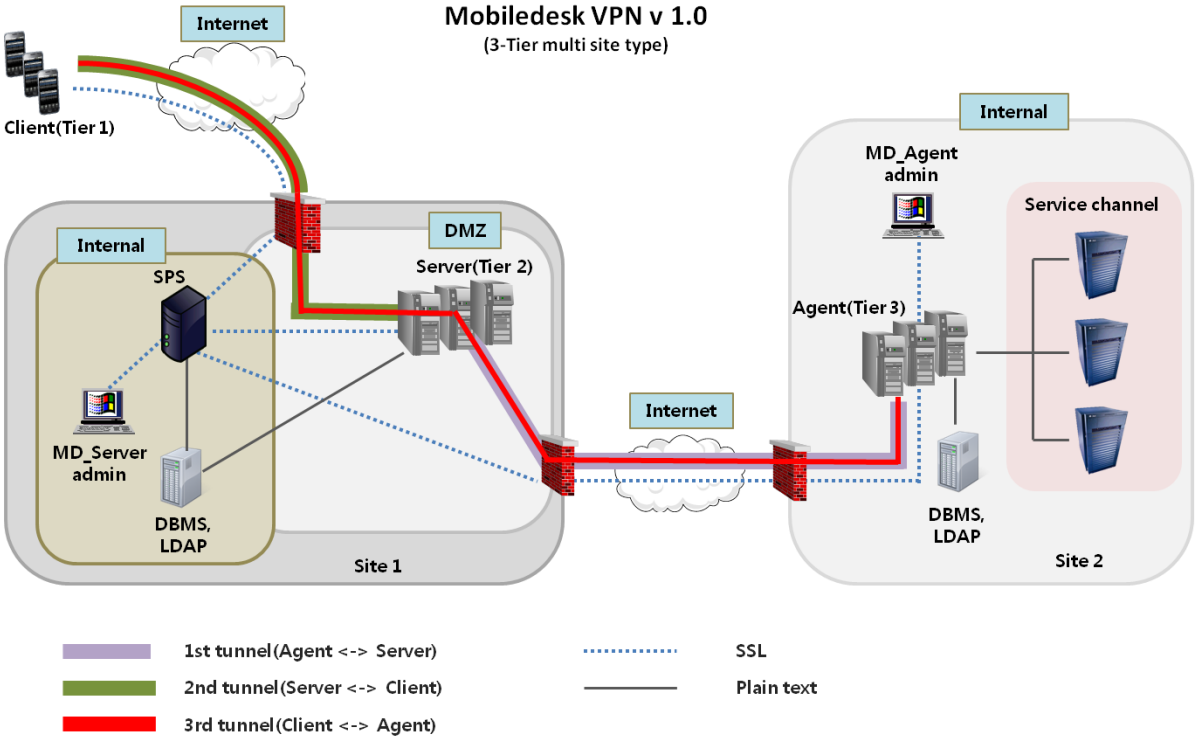
■ Operational Environment for the TOE

The TOE can have three kinds of operational environments according to the networking environment of the MD_Server, MD_SPS, and MD_Agent: the Multiple Site Type and the Single Site Type. The Single Site Type can be again classified into 3Tier and 2Tier depending on the existence of the MD_Server.

• Multiple Site Type

The Multiple Site Type is the TOE operational environment that the MD_Server and the MD_SPS form the core that connects with many MD_Agents operated in an independent network environment. The Multiple Site Type establishes three kinds of tunneling to protect communications between the MD_Server and the MD_Agent (the 1st tunneling), between the MD_Server and the MD_Client (the 2nd tunneling), and between the MD_Client and the MD_Agent (the 3rd tunneling).

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved



[Figure 1] TOE operational environment (Multiple Site Type)

The client user on the internet can ultimately access to the web or DB services provided by the Internal Network of the Site 2 using VPN communication through the 3rd tunneling. The audit data generated by the MD_SPS and the MD_Agent is stored in the DMBS managed through the MD_SPS and the MD_Agent respectively. [1] The TOE uses VPN tunneling provided by the TOE itself to protect transmitted user data, and also uses SSL tunneling provided by the operational environment to protect communications between the authorized administrator's (the MD_Agent administrator or the MD_Server administrator) PC and the MD_Agent or MD_SPS/MD_Server. Additionally, the MD_Agent and the mobile device for the MD_Client must be registered to the MD_SPS beforehand to use them for VPN

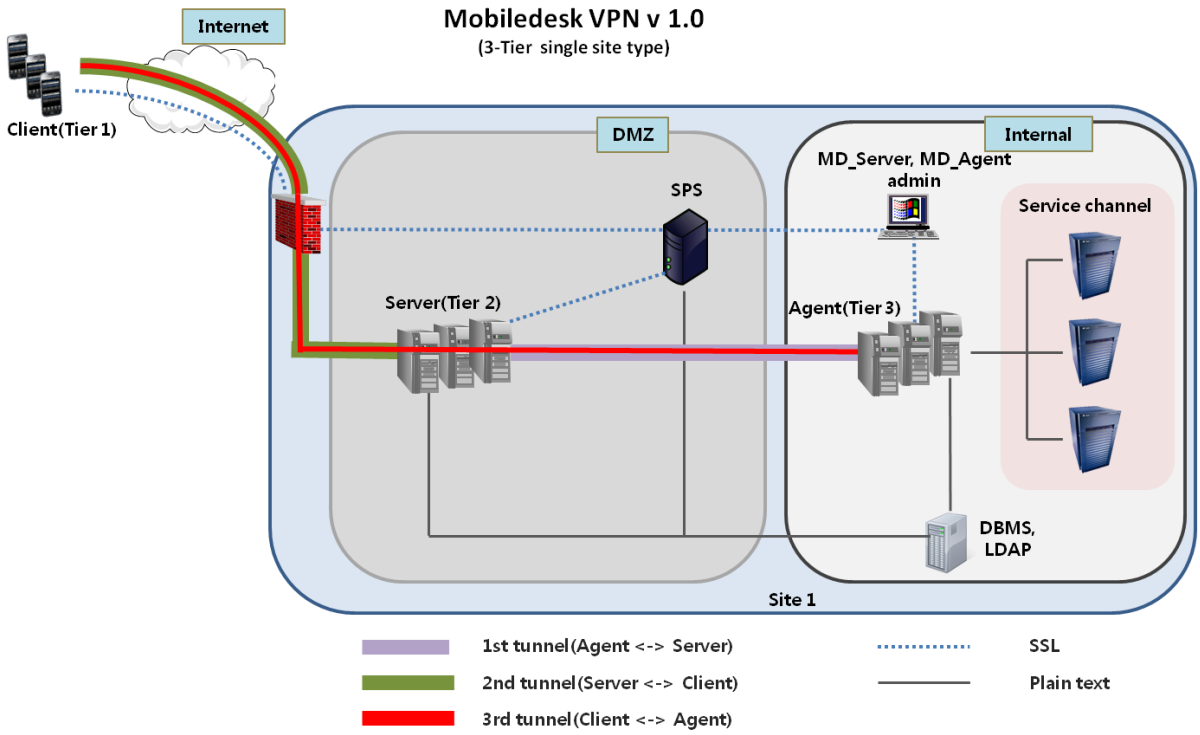
[1] Audit records of auditable events related to the VPN communication connection are stored in a file, whereas audit records of the other events are stored in the DBMS.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

communication, the TOE also uses SSL tunneling provided by the operational environment to protect transmitted data during registration.

• 3Tier Single Site Type

The 3Tier Single Site Type is the TOE operational environment that the MD_Server, the MD_SPS, and the MD_Agent are operated on the same network. The MD_Server and the MD_SPS exist in the DMZ network while the MD_Agent exists in the internal network. The 3Tier Single Site Type establishes three kinds of tunneling to protect communications between the MD_Server and the MD_Agent (the 1st tunneling), between the MD_Server and the MD_Client (the 2nd tunneling), and between the MD_Client and the MD_Agent (the 3rd tunneling).



[Figure 2] TOE operational environment (3Tier Single Site Type)

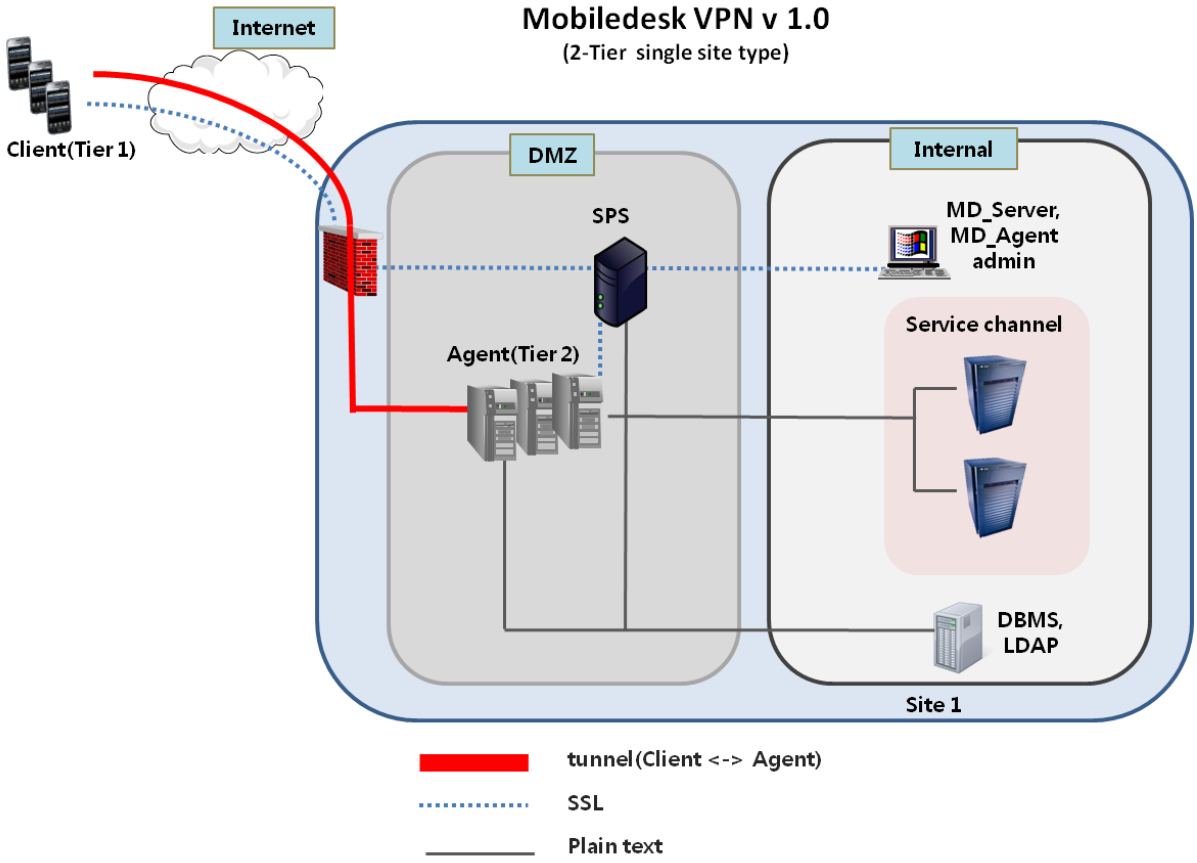
Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

The client user on the internet can ultimately access to the web or DB services provided by the Internal Network of the Site 1 using VPN communication through the 3rd tunneling. The audit data generated by the MD_SPS and the MD_Agent is stored in the DMBS, and the MD_Server administrator and the MD_Agent administrator can only access audit data generated by each TOE component respectively.

• 2Tier Single Site Type

The 2Tier Single Site Type is the TOE operational environment that the MD_SPS and the MD_Agent are operated on the same network environment without the MD_Server. The MD_SPS and the MD_Agent exist in the DMZ network of the network environment. The 2Tier Single Site Type establishes only one tunneling to protect communications between the MD_Client and the MD_Agent (the 3rd tunneling).

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved



[Figure 3] TOE operational environment (2Tier Single Site Type)

The client user on the internet can ultimately access to the web or DB services provided by the Internal Network of the Site 1 using VPN communication through the 3rd tunneling. The audit data generated by the MD_SPS and the MD_Agent is stored in the DMBS, and the MD_Server administrator and the MD_Agent administrator can only access audit data generated by each TOE component respectively.

■ Major Security Features of the TOE

The TOE provides the Mobile-Based VPN and the other additional security features such as security management for VPN communication, user identification and authentication, security audit, failure detection for the TOE main processes, and testing of external

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

entities.

■ **Mobile-Based VPN**

The TOE protects transmitted user data amongst the TOE components using cryptographic operations through the 1st, the 2nd, and the 3rd tunneling.

• **Cryptographic Modules**

In order to protect transmitted data between the TOE components, the TOE implements security features by utilizing validated cryptographic modules under Korean Cryptographic Module Validation Program. The used cryptographic modules according to TOE components and the operating systems are listed in the following table.

TOE Component	Validated Crypto Module	OS
MD_Client (application, library)	MaxigentCrypto V1.0 (Samsung SDS)	Android 2.2 Android 2.3 iOS 4.3
MD_Server	SNIPER Crypto V1.2 (WINS Technet CO., Ltd)	RedHat Enterprise Linux 5 (Kernel 2.6)(32bit/64bit)
MD_Agent	SNIPER Crypto V1.2 (WINS Technet CO., Ltd)	RedHat Enterprise Linux 5 (Kernel 2.6)(32bit/64bit)
	- [2]	Windows Server 2003(32bit/64bit) Windows Server 2008(32bit/64bit)

[Table 3] Cryptographic Module

[2] The MD_Agent doesn't utilize validated cryptographic modules when it is installed on the Windows Server 2003/2008. Instead it uses cryptographic functions implemented in it for VPN communication.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

• **Tunneling**

The TOE establishes VPN tunneling between TOE components to connect the Mobile-Based VPN communication as following.

Multiple Site Type and 3Tier Single Site Type	
1st Tunneling	The tunneling section between the MD_Agent and the MD_Server.
2nd Tunneling	The tunneling section between the MD_Client and the MD_Server.
3rd Tunneling	The tunneling section between the MD_Client and the MD_Agent. As the 3rd tunneling is established using the 1st and the 2nd tunneling, it can only be created after successful the 1st and the 2nd tunneling establishment.

[Table 4] Tunneling (Multiple Site Type and 3Tier Single Site Type)

2Tier Single Site Type	
3rd Tunneling	The tunneling section between the MD_Client and the MD_Agent.

[Table 5] Tunneling (2Tier Single Site Type)

■ **Protected Assets of the TOE**

Assets that TOE must protect are user data transmitted through TOE components, and also include TOE itself and the security critical data (security attributes, cryptographic

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

keys[3], TSF data, etc.) of the TOE.

1.3.2 Required non-TOE Hardware/Software

■ **Required non-TOE Hardware Platform**

TOE Component	Platform	Category	Recommended Specifications
MD_Agent	Server	CPU	Pentium 4 2.6GHz or higher (Quad core or higher)
		RAM	4GB or higher
		HDD	30GB or higher
		NIC	One unit of 10/100/1000Mbps
MD_Server	Server	CPU	Pentium 4 2.6GHz or higher (Quad core or higher)
		RAM	4GB or higher
		HDD	64GB or higher
		NIC	One unit of 10/100/1000Mbps
MD_SPS	Server	CPU	Pentium 4 2.6GHz or higher (Quad core or higher)
		RAM	4GB or higher
		HDD	30GB or higher
		NIC	One unit of 10/100/1000Mbps
MD_Client	Mobile Device (Android) Samsung, LG,	CPU	ARMv7 720MHz or higher
		RAM	512MB or higher
		Memory	8GB or higher

[3] The TOE generates and uses session keys (for ARIA and SEED symmetric keys, and HMAC key) for VPN communication connection for each time, and the TOE manages cryptographic keys used in VPN communication. Private key/public key pairs used for registered mobile device and MD_Agent check, and server authentication are securely generated and managed by the IT environment. (See section 1.3.2 Required non-TOE Software - JCE Library and OpenSSL, and section 1.6 Terminology).

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

TOE Component	Platform	Category	Recommended Specifications
	Motorola, HTC	Network	3G Network(HSDPA) or Wi-Fi 802.11 b/g/n supported
	Mobile Device (iOS)	CPU	ARMv7 833Mhz or higher
		RAM	256 MB or higher
		Memory	8GB or higher
		Network	3G Network(HSDPA) or Wi-Fi 802.11 b/g/n supported

[Table 6] Required non-TOE hardware platform

■ **Required non-TOE OS**

TOE Component	OS	
MD_Agent	Multiple Site Type	RedHat Enterprise Linux 5(Kernel 2.6)(32bit/64bit)
	3Tier Single Site Type	Windows Server 2003(32bit/64bit) Windows Server 2008(32bit/64bit) RedHat Enterprise Linux 5(Kernel 2.6)(32bit/64bit)
	2Tier Single Site Type	RedHat Enterprise Linux 5(Kernel 2.6)(32bit/64bit)
MD_Server	RedHat Enterprise Linux 5(Kernel 2.6)(32bit/64bit)	
MD_SPS	Windows Server 2003(32bit/64bit) Windows Server 2008(32bit/64bit)	
MD_Client	Android	Android 2.2, Android 2.3
	iOS	iOS 4.3

[Table 7] Required non-TOE OS

■ **Required non-TOE Software**

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

• **Web Browser (Internet Explorer 7.0/8.0)**

The MD_Server administrator and the MD_Agent administrator performs security management of the MD_Server and MD_Agent respectively using Internet Explorer 7.0 or 8.0 which are provided by the administrator's PC.

• **Web Application Server (Tomcat 6.0)**

Tomcat 6.0, web application server provided by operational environment of the MD_SPS and the MD_Agent, provides the environment for the MD_Server administrator and the MD_Agent administrator to access TOE through the web browser so that they can perform security management of the TOE.

• **SSL Library (Java Secure Socket Extension (JSSE) 1.6)**

JSSE 1.6, SSL library provided by operational environment JDK 6, provides secure communication between web browser on the administrator's PC and TOE when the authorized administrator performs security management of the TOE.

The MD_Agent and the mobile device for the MD_Client must be registered to the MD_SPS beforehand to use them for VPN communication, JSSE 1.6 also provides secure communication between the MD_SPS and TOE components during registration.

• **JCE Library (Java Cryptography Extension 1.6)**

JCE 1.6, Java cryptographic library provided by operational environment, provides cryptographic services as following:

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

- MD_Client: MD_Client reg. private key/public key generation, and encryption/decryption of the generated MD_Client reg. private key, password, and configuration file,
- MD_Agent: MD_Agent reg. private key/public key generation, private key/public key generation for server authentication, and encryption/decryption of the license file including generated MD_Agent reg. private key,
- MD_Server: private key/public key generation for server authentication,
- MD_SPS: encryption of the MD_Agent license file to be transmitted.

JCE 1.6 is provided by Android OS for the MD_Client and JDK 6 for the MD_Agent and the MD_SPS.

• OpenSSL (OpenSSL 1.0.0d)

OpenSSL provided by operational environment of MD_Client library for iOS generates MD_Client reg. private key/public key.

• LDAP (Apache Directory Server 1.5.7, Oracle Directory Server Enterprise Edition 11g, SUN Directory Server Enterprise Edition 6.0)

LDAP (Lightweight Directory Access Protocol) provided by operational environment is utilized by the MD_Server to manage VPN session and the MD_SPS information, and by the MD_SPS to manage the MD_Agent and the MD_Client information (mobile device ID, the MD_Agent and MD_Client reg. public keys). Similarly, the MD_Agent which is installed and operated on the Linux OS utilizes LDAP to manage the MD_Client information (client user reg. ID/password, mobile device ID, the MD_Client reg. public key).

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

• **DBMS (Oracle 10g, Microsoft SQL Server 2005)**

DBMS, which is provided in the operational environment, is utilized by the MD_Agent and the MD_SPS to store and protect generated audit data. Also, the MD_Agent utilizes DBMS to store and protect security critical TSF data (user group, the Mobile-Based VPN user privilege, service channel information, configuration parameters, VPN connection status information).

Required non-TOE hardware, OS, web browser, WAS, JSSE, JCE, OpenSSL, LDAP, and DBMS are out of the TOE scope.

1.3.3 References

The TOE is developed based on the RFCs related to the standard SSH by IETF (Internet Engineering Task Force). See list of RFCs below.

RFC No.	RFC Title
4251	The Secure Shell (SSH) Protocol Architecture.
4252	The Secure Shell (SSH) Authentication Protocol.
4253	The Secure Shell (SSH) Transport Layer Protocol.
4254	The Secure Shell (SSH) Connection Protocol.
4256	Generic Message Exchange Authentication for the Secure Shell (SSH).

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The physical scope of the TOE includes following TOE components and related guidance documents. [4]

TOE Component	TOE Component Identifier and Build Version	Delivery Form
MD_Agent	Mobiledesk VPN Agent for Linux v1.0.5 Mobiledesk VPN Agent for Windows v1.0.5	Setup File
MD_Server	Mobiledesk VPN Server v1.0.5	
MD_SPS	Mobiledesk VPN SPS v1.0.5	
MD_Client	Mobiledesk VPN Client for Android v1.0.4	
	Mobiledesk VPN Client Library for Android v1.0.4 Mobiledesk VPN Client Library for iOS v1.0.4	Library
Guidance Documents	Mobiledesk VPN v1.0 Agent Manual v1.1 Mobiledesk VPN v1.0 Server Manual v1.1 Mobiledesk VPN v1.0 Client Manual v1.1 Mobiledesk VPN v1.0 Developer Manual v1.0	Softcopy

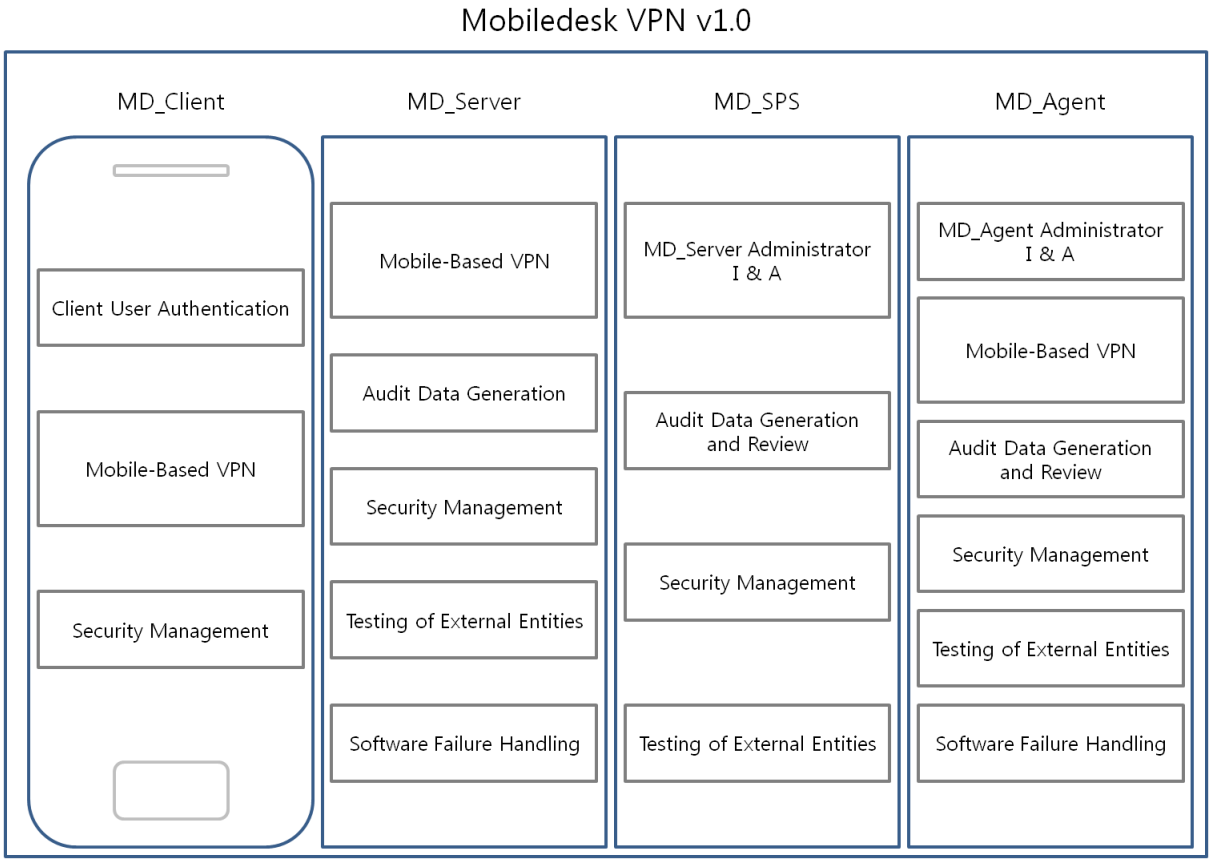
[Table 8] Physical scope of the TOE

1.4.2 Logical Scope of the TOE

The figure below shows the major security features provided by TOE.

[4] The organization which operates the TOE after the TOE delivery by developer distributes the MD_Client to the users inside of the organization, the organization is responsible for this internal distribution, and out of the TOE evaluation.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved



[Figure 4] Logical Scope of the TOE

• **Client user authentication**

Client users must authenticate themselves to the MD_Client to use it by providing password registered during initial start-up after installation of the MD_Client.

• **Mobile-Based VPN**

The TOE provides the Mobile-Based VPN through tunneling connection to protect data transmitted between the MD_Server and the MD_Agent (the 1st tunneling), the MD_Server and the MD_Client (the 2nd tunneling), and the MD_Client and the MD_Agent (the 3rd tunneling). The TOE controls information flows amongst TOE

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

components using the Mobile-Based VPN policy based on security attributes, and provides VPN functions by standard cryptographic services such as cryptographic key generation and distribution, cryptographic key destruction, and cryptographic operations.

To establish the VPN connection, the TOE verifies fingerprint for server authentication, conducts key exchangement, and checks if a TOE component which plays a VPN client role is allowed peer to the other TOE component which plays a VPN gateway server.

When the client user doesn't interact with the MD_Client for a certain time period (280 seconds ~ 300 seconds, up to the networking environment of the MD_Client), the TSF terminates the VPN session.

• Audit Data Generation and Review

The TOE generates audit data for security related events. Audit data generated by the TOE is classified according to TOE components: MD_Server Log, MD_SPS Log, and MD_Agent Log. And audit data includes audit records about VPN connection amongst TOE components, identification and authentication of authorized administrators (the MD_Server administrator and the MD_Agent administrator) for security management, and use of the security management functions. Audit records about VPN connection are stored in files, and the others are stored in the DBMS. The MD_Server administrator and the MD_Agent administrator are allowed to review MD_Server and MD_SPS Log, and MD_Agent Log respectively.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

• **MD_Server administrator I & A**

The MD_SPS identifies and authenticates the MD_Server administrator who can conduct security management. The MD_Server administrator accesses to the MD_SPS using web browser (HTTPS), the IP address of the administrator's PC and the entered ID/password are verified against those in the DBMS. When 3 of consecutive unsuccessful authentication attempts have been met, the account is locked for a certain time period (10 minutes) to prevent further authentication.

• **MD_Agent administrator I & A**

The MD_Agent identifies and authenticates the MD_Agent administrator who can conduct security management. The MD_Agent administrator accesses to the MD_Agent using web browser (HTTPS), the IP address of the administrator's PC and the entered ID/password are verified against those in the DBMS. When 3 of consecutive unsuccessful authentication attempts have been met, the account is locked for a certain time period (10 minutes) to prevent further authentication.

• **Security Management**

The MD_Server administrator can manage the MD_Server and the MD_SPS after successful identification and authentication to the MD_SPS. The MD_Server is managed only through the MD_SPS. The MD_Server administrator can manage security attributes and the TSF data necessary to operate the MD_Server and the MD_SPS, and information related to the MD_Agent and the MD_Client to establish VPN connection between TOE components.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Similarly, the MD_Agent administrator can manage the MD_Agent after successful identification and authentication to the MD_Agent. The MD_Agent administrator can register the MD_Agent to conduct VPN communication to the MD_SPS, and manage security attributes and the TSF data necessary to operate the MD_Agent, and information released to the client user and the MD_Server to establish VPN connection with the MD_Agent.

During the MD_Agent registration the MD_Agent reg. ID/password[5] is checked, and the MD_Agent reg. public key is stored in the LDAP through the MD_SPS for future use in the Mobile-Based VPN policy.

The client user can register the MD_Client installed mobile device to use VPN communication to the MD_SPS and the MD_Agent, and set password and configuration parameters for VPN communication after successful authentication to the MD_Client.

During mobile device registration the client user reg. ID/password[6] is checked, and the MD_Client installed mobile device ID and the MD_Client reg. public keys are stored in the LDAP through the MD_SPS and the MD_Agent for future use in the Mobile-Based VPN policy.

Also, the TSF terminates the administrator's session when the MD_Server administrator and the MD_Agent administrator don't interact with the MD_SPS and the MD_Agent for a certain time period (10 minutes).

[5] The MD_Server administrator generates the MD_Agent reg. ID/password to the MD_SPS.

[6] The MD_Agent administrator generates the client user reg. ID/password to the MD_Agent, the client user can register the MD_Client installed mobile device to the MD_SPS and the MD_Agent using this ID/password.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

• **Software Failure Handling**

The MD_Server and the MD_Agent run the daemon that checks their own running status regularly, and handle software failure by restarting the process which is abnormally terminated.

• **Testing of External Entities**

The TOE provides testing of external entities (WAS, LDAP, and DBMS) whenever it requests to these external entities for services (call for web pages to the WAS, request for the data stored in the LDAP, and query request to the DBMS).

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

1.5 Conventions

This Security Target uses English for certain abbreviations and to accurately convey the meanings. Used notations, forms, and drafting rules follow the Common Criteria. The Common Criteria allows the operations of iteration, Assignment, Selection, and refinement that may be performed in security requirements. Each operation is used in this Security Target.

- **The iteration operation**

  Use of the same component to express two or more distinct requirements.

  The results of the iteration operation are expressed as the iteration number in parentheses after the component identifier, i.e. (Iteration number).

- **The assignment operation**

  The specification of an identified parameter in a component or requirement.

  The results of the assignment operation are placed in large brackets, i.e. [Allocation value].

- **The selection operation**

  Specification of one or more items from a list in a component.

  The results of the selection operation are *italicized and underlined*.

- **The refinement operation**

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Addition of details to a component.

The results of the refinement operation are in **bold text**.

This Security Target provides *"Application Note"* to clarify the meanings of the requirements.

The cautions are provided with the corresponding requirements if necessary.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

1.6 Terminology

Object

Passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Identity

Representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE

Authentication Data

Information used to verify the claimed identity of a user

Element

Indivisible statement of a security need

Operation (on a component of the CC)

Modification or repetition of a component

Operation (on an object)

Specific type of action performed by a subject on an object

External Entity

Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Asset

Entities that the owner of the TOE presumably places value upon.

Organizational Security Policies

Set of security rules, procedures, or guidelines for an organization

Dependency

relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Subject

Active entity in the TOE that performs operations on objects

Component

Smallest selectable set of elements on which requirements may be based

Class

Set of CC families that share a common focus

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

Evaluation Assurance Level (EAL)

Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Extension

Addition to an ST or PP of functional requirements not contained in CC Part 2 and/or assurance requirements not contained in CC Part 3

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

TOE Security Functionality (TSF)

Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

Mobile-Based Virtual Private Network

VPN is a communication service that can use public networks such as the internet network as private networks and save the costs considerably. It allows the internet network to be used as a private network by providing special communication system and cryptographic technique. The Mobiledesk VPN provides VPN that is run on mobile devices.

Multiple Site Type

A type of operational environment for the Mobiledesk VPN. Multiple MD_Agents which are located in an independent network can be connected to the MD_Server. The MD_Client establishes the Mobile-Based VPN with the MD_Agent through MD_Server. Each MD_Agent can be operated using a private IP address.

3Tier Single Site Type

A type of operational environment for the Mobiledesk VPN. The MD_Server and the MD_Agent are located and connected in the same network. The MD_Client establishes the Mobile-Based VPN with the MD_Agent through MD_Server. Each MD_Agent can be operated using a private IP address.

2Tier Single Site Type

A type of operational environment for the Mobiledesk VPN. In the Mobile-Based VPN policy, the MD_Client and the MD_Agent are directly connected without the MD_Server. Each MD_Agent can only be operated using a public IP address.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

3Tier Operational environment

In the 3Tier operational environment, 3 TOE components (the MD_Client, the MD_Server, and the MD_Agent) are involved to establish 3 kind of tunneling (the 1st, the 2nd, and the 3rd tunneling) based on the Mobile-Based VPN policy. This includes the Multiple Site Type and the 3Tier Single Site Type.

2Tier Operational environment

In the 2Tier operational environment, 2 TOE components (the MD_Client and the MD_Agent) are involved to establish one tunneling (the 3rd tunneling) based on the Mobile-Based VPN policy. This includes the 2Tier Single Site Type.

1st Tunneling

Tunneling between the MD_Agent and the MD_Server based on the Mobile-Based VPN policy.

2nd Tunneling

Tunneling between the MD_Client and the MD_Server based on the Mobile-Based VPN policy.

3rd Tunneling

Tunneling between the MD_Client and the MD_Agent based on the Mobile-Based VPN policy.

MD_Server (Mobiledesk VPN Server)

A server program installed on the server platform. It manages information related to the MD_Client and the MD_Agent, and connects and acts as a relay server among TOE components. In this Security Target, both notations MD_Server and Mobiledesk VPN server are used.

MD_Client (Mobiledesk VPN Client)

The MD_Client is provided as an application or a library. In this Security Target, both

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

notations MD_Client and Mobiledesk VPN Client are used.

- Mobiledesk VPN Client Application

A client program installed on the mobile device. It acts as a VPN client by connecting the client user to the MD_Agent. In the ST, The MD_Client refers to the 'MD_Client application' unless it is denoted as 'library'.

- Mobiledesk VPN Client Library

A set of client library used to develop a client program installed on the mobile device.

MD_Agent (Mobiledesk VPN Agent)

The MD_Agent is installed on the server platform and provides VPN gateway server for client users. It is an agent program that manages the log-in of the client users and the connection between the client user and the server that provides internal network service channel. In this Security Target, both notations MD_Agent and Mobiledesk VPN agent are used.

MD_SPS (Mobiledesk VPN Service Provisioning Server)

It is installed on the server platform and registers information related to the MD_Client installed mobile device and the MD_Agent so that they can be applied to the MD_Server and MD_Agent for the VPN function. It also manages configuration parameters for the MD_Server, and plays a role as trusted authentication server for server authentication. In this Security Target, both notations MD_SPS and Mobiledesk VPN Service Provisioning Server are used.

Client Developer

Developer that develops VPN client program using the MD_Client library

Client User

User that receives/transmits information on the mobile device through TOE

Authorized Administrators

Authorized user who safely operates and manages the MD_Agent, the MD_Server, and

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

the MD_SPS according to the TOE security policies. It includes the MD_Server administrator and the MD_Agent administrator.

MD_Agent Administrator

Authorized user who manages the MD_Agent according to the TOE security policies after successful authentication

MD_Server Administrator

Authorized user who manages the MD_Server and the MD_SPS according to the TOE security policies after successful authentication

Private Key

A secret key used in asymmetric cryptography. It is mathematically equivalent to a public key, but is kept secret.

The TOE uses several private/public key pairs for server authentication and registered MD_Agent and MD_Client check.

Public Key

A publically distributed key used in asymmetric cryptography. It is mathematically equivalent to a private key, but is widely distributed.

The TOE uses several private/public key pairs for server authentication and registered MD_Agent and MD_Client check. It is also referred as host key if it is used for server authentication.

Server Authentication

The method to authenticate the component which plays a server role by the component which plays a client role when establishing the Mobile-Based VPN connection between TOE components. The server transmits fingerprint of the server public key to the client during client registration. For each VPN connection, the server transmits the server public key to the client, and the client verifies fingerprint of the public key (host key).

The MD_Server plays the server role in the 3Tier operational environment, and the

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

MD_Agent in the 2Tier operational environment. Each Private/public key pair for the MD_Server and the MD_Agent for server authentication is generated by JCE which is operational environment.

MD_Client Reg. Private Key, MD_Client Reg. Public Key

The MD_Client must be checked if it is authorized or not during establishment of the Mobile-Based VPN connection with the MD_Server or the MD_Agent, and the MD_Client reg. private key and public key pairs generated by JCE which is operational environment are used for this checking (two private/public key pairs are generated for both the MD_Server and the MD_Agent). The process is completed by simply comparing the public key transmitted by the MD_Client with the public key stored in the MD_Server or the MD_Agent side. During mobile device registration, the MD_Client reg. private key is stored in the MD_Client, the MD_Client reg. public key is delivered and stored in the MD_Server and the MD_Agent.

MD_Agent Reg. Private Key, MD_Agent Reg. Public Key

The MD_Agent must be checked if it is authorized or not during establishment of the Mobile-Based VPN connection with the MD_Server, and the MD_Agent reg. private key and public key pairs generated by JCE which is operational environment are used for this checking. The process is completed by simply comparing the public key transmitted by the MD_Agent with the public key stored in the MD_Server side. During the MD_Agent registration, the MD_Agent reg. private key is included in the license file and stored in the MD_Agent, the MD_Agent reg. public key is delivered and stored in the MD_Server.

Mobile Device Registration

It refers to the process of storing the mobile device information (Mobile Device ID, the MD_Client Reg. Public Key) in the MD_Server and the MD_Agent before using the Mobile-Based VPN provided by mobile devices installed with the MD_Client.

MD_Agent Registration

It refers to the process of storing the information of the MD_Agent (MD_Agent reg.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

public key) in the MD_Server before using the Mobile-Based VPN provided by the MD_Agent.

Remote Port Forwarding

The MD_Client connects to a local port, and then the MD_Server's port which is agreed between the MD_Agent and the MD_Server to communicate with the MD_Agent, the MD_Server retransmits incoming packets to its port to the MD_Agent which is assigned to that port.

License File

It is a license file that is provided by the MD_SPS to use the MD_Agent after the installation of the MD_Agent, and includes information related to the MD_Agent reg. ID, the MD_Agent reg. private key, expiration date, and the number of users, in an encrypted file.

Client User Reg. ID/Password

It is information that is used to check the client user during mobile device registration. It is created by the MD_Agent administrator and stored in the MD_Agent.

MD_Agent Reg. ID/Password

It is information that is used to check the MD_Agent during the MD_Agent registration. It is created by the MD_Server administrator and stored in the MD_SPS. Also, the MD_Agent reg. ID is used to check the MD_Agent itself to the MD_Server right after establishment of VPN connection.

Client User Role

A Category used to group many client user reg. IDs. It is used to set the MD_Client authorization to access service channels provided by the MD_Agent.

Mobile Device ID

ID composed of 15 digit numbers. It has unique values for each mobile device (mobile

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

device), and is used to identify the mobile devices (mobile device). Also, the mobile device ID is used to check the MD_Client itself to the MD_Server or the MD_Agent right after establishment of VPN connection.

Service Channel

Services (web, DB and so on) provided by the internal network that the MD_Client can access through the MD_Agent after successful establishment of tunneling for the Mobile-Based VPN

Encryption

A process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key

Decryption

A reverse process of encryption

Server Platform

Computer that is installed with the recommended hardware and OS as specified in the Security Target

Mobile Device

Mobile device that is installed with the MD_Client

The Third Generation Network

It is a network for mobile phones and supports high speed data communication as well as regular voice telephony through the third generation mobile phone method.

WI-FI(Wireless-Fidelity)

Wireless network LAN standard that uses 2.4 GHz

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Application

A form of the MD_Client. The MD_Client application is independently started, stopped, and run by the client user in the mobile device.

Library

A form of the MD_Client. The MD_Client library is included in the other external entity (e.g., a VPN client) to be started, stopped, and run by the client user in the mobile device.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

2. Conformance Claims

This chapter shows how the Security Target conforms to the Common Criteria, Protection Profile and Package.

2.1 Common Criteria Conformance Claim

This Security Target conforms to the following Common Criteria.

- **CC Identification**

  - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1r3, 2009. 7, CCMB-2009-07-001

  - Common Criteria for Information Technology Security Evaluation, Part 2: Requirements for Security Functions, Version 3.1r3, 2009. 7, CCMB-2009-07-002

  - Common Criteria for Information Technology Security Evaluation, Part 3: Assurance Requirements, Version 3.1r3, 2009. 7, CCMB-2009-07-003

- **CC Conformance**

  - Part 2 conformant

  - Part 3 conformant

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

2.2 Protection Profile Claim

This Security Target does not conform to any Protection Profile.

2.3 Package Claim

This Security Target conforms to the following Package.

- **Assurance Package: EAL3 conformant**

2.4 Conformance Rationale

Because this Security Target does not conform to any Protection Profiles, conformance rationale is not necessary.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

3. Security Problem Definition

Security problem definition defines the threats, organizational security policies, and assumptions that are to be addressed by the TOE and its operational environment .

3.1 Threats

Attackers are IT entities or human users who try to compromise the confidentiality and the integrity of user data[7] transmitted between TOE components, illegally access to the TOE in order to perform adverse action to the TOE. Attackers are assumed to have a basic level of expertise, resources, and motivation.

T.UNAUTH.ACCESS	An attacker may illegally access or modify user data transmitted between TOE components.
T.ADMIN.DISGUISE	An attacker may access to the management function of the TOE by disguising as authorized administrator (the MD_Agent administrator and the MD_Server administrator).
T.CUSER.DISGUISE	An attacker may access to the service provided by the MD_Client by disguising as client user.
T.REPEAT.AUTH	An attacker may acquire the authorized administrator (the MD_Agent administrator and the MD_Server administrator) rights by repeatedly attempting authentication to access to the management function of the TOE.

[7] Topology data such as IP address and port number are not included in user data that the TOE handles.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

T.SW.FAILURE	An attacker may try to lead software failure such as the TOE's critical process runtime errors so that the TOE cannot provide normal services to users.
T.DISABLE.EXT	An attacker may disable the external entities necessary for the TSF operation so that the TOE cannot provide normal services to users.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

3.2 Organizational Security Policies

This section describes the organizational security policies that apply to the TOE.

P.MOBILE.VPN	The TOE shall enforce the Mobile-Based VPN policy to control information flows of user data transmitted between TOE components. - The TOE only allows information flows provided with confidentiality, integrity and authentication using VPN connection. - The TOE only allows information flows between TOE components that are allowed to use VPN connection.
P.CRYPTO	The TOE shall perform cryptographic key management and operations according to the national or international standard to protect user data transmitted between TOE components based on the Mobile-Based VPN policy.
P.AUDIT	Security relevant events shall be recorded and maintained to trace security related actions, and the recorded data shall be reviewed.
P.MANAGEMENT	The TOE shall provide management measures to securely manage the TOE to authorized administrators (the MD_Agent administrator and the MD_Server administrator) and client users. Each role can manage

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

following TOE components:

Role	TOE component
MD_Agent administrator	MD_Agent
MD_Server administrator	MD_Server MD_SPS
Client User	MD_Client

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

3.3 Assumptions

This section describes the assumptions that are made on the operational environment in order to be able to provide security functionality.

A.PHYSICAL	The MD_Server, the MD_SPS and the MD_Agent are located in a physically secure environment of customer's site so that they are protected from physical access.
A.ADMIN	Authorized administrators are non-hostile and properly trained about the TOE management function, and follow all administrator guidance.
A.CUSER	Client users are non-hostile and properly trained about the TOE usage. Also, client users don't disclose the authentication data necessary for the TOE usage, and are responsible for physical security of the mobile device with the MD_Client. *Application note*: Client users take proper actions in case of the lost mobile device by informing authorized administrator to prevent to use VPN services provided by the MD_Client.
A.CLIENT.DISTRIBUTION	The organization that uses the TOE is responsible for the secure distribution of the MD_Client to client users.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

A.OS	The operating system underlying the MD_Server, the MD_SPS, and the MD_Agent is enhanced by managing it (e.g., patching it due to vulnerabilities) so that it provides secure computing environment. And the OS provides audit storage and timestamp necessary for the TOE's audit records for security relevant events. *Application note: Audit data related to the VPN connection is stored in files and the protection of the audit trail is provided by the OS. In addition to the TOE generates audit records using time source from the OS.* The operating system for the MD_Client is official version provided by mobile device vendors. *Application note: The mobile device for the MD_Client is free from unauthorized modification such as rooting or jailbreaking.*
A.OP.POLICY	The TOE operation environment is maintained according to the networking environment such as increase/decrease of the hosts or services.
A.MANAGEMENT.COMM	The web application server (WAS) provided by the operational environment of the TOE provides the environment for authorized administrators (the

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	MD_Server administrator and the MD_Agent administrator) to access the TOE through the web browser so that they can perform security management of the TOE. SSL library provided by operational environment of the TOE provides secure communication between web browser on the administrator's PC and TOE when the authorized administrator performs security management of the TOE. The MD_Agent and the mobile device for the MD_Client must be registered to the MD_SPS beforehand to use them for VPN communication, SSL library also provides secure communication between the MD_SPS and TOE components during registration.
A.CRYPTO	Java cryptographic library and OpenSSL provided by operational environment of the TOE provides cryptographic services for secure TOE operation. Also, private key/public key pairs used by the TOE for registered mobile device and MD_Agent check, and sever authentication are securely generated and managed by IT environment.
A.DATA.REG	The MD_Agent administrator stores the client user

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	reg. ID/password to the DBMS through the MD_Agent, and securely delivers them to the client user. The MD_Server administrator stores the MD_Agent reg. ID/password to the DBMS through the MD_SPS, and securely delivers them to the MD_Agent administrator.
A.DBMS	The DBMS provided by operational environment of the TOE stores and maintains TSF data and audit data necessary for the operation of the TOE. The DBMS administrator from the organization that uses the TOE is responsible for secure operation of the DBMS. *Application note: All audit data except for those related to the VPN connection is stored in the DBMS.*
A.LDAP	The LDAP provided by operational environment of the TOE provides the environment for management of the data necessary for the Mobile-Based VPN policy of the TOE.
A.NETWORKING.DEVICE	There exist various networking devices to support operation of the TOE according to the various TOE operational environment type of the customer site,

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

and the internal network of the organization is protected by network boundary protection devices such as firewall.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

4. Security Objectives

This section describes security objectives divided into two part wise solutions. Security objectives for the TOE are security objectives addressed by the TOE, and security objectives for the operational environment implements technical and procedural measures to assist the TOE in correctly providing its security functionality.

4.1 Security Objectives for the TOE

O.AUDIT	The TOE must record security related events to trace security relevant actions, provide measures to review recorded data.
O.DATA.PROTECTION	The TOE must protect confidentiality and integrity of user data transmitted between TOE components by performing cryptographic key management and operations according to the national or international standard.
O.ADMIN.I&A	The TOE must uniquely identify the MD_Agent administrator and the MD_Server administrator as authorized administrators, and authenticate them before allowing them access to the TOE to use management function of the TOE. The TOE must take proper actions for unsuccessful authentication.
O.CUSER.AUTH	The TOE must authenticate the client user before allowing them access to the TOE to use and manage the MD_Client.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

O.VPN.POLICY	The TOE must control information flows between TOE components according to the Mobile-Based VPN policy.
O.MANAGEMENT	The TOE must provide management measures to securely manage the TOE to the authorized administrator and the client user.
O.SECURE.STATE	The TOE must maintain secure state in case of software failure such as the TOE's critical process runtime errors.
O.TESTING.EXT	The TOE must conduct testing of external entities, necessary for the TSF operation, interacting with the TOE.

4.2 Security Objectives for the Operational Environment

OE.PHYSICAL	The MD_Server, the MD_SPS and the MD_Agent are located in a physically secure environment of customer's site so that they are protected from physical access.
OE.ADMIN	Authorized administrators are non-hostile and properly trained about the TOE management function, and follow all administrator guidance.
OE.CUSER	Client users are non-hostile and properly trained about the TOE usage. Also, client users don't disclose the authentication data necessary for the TOE usage, and are responsible for physical security of the mobile device with the MD_Client.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

OE.CLIENT.DISTRIBUTION	The organization that uses the TOE is responsible for the secure distribution of the MD_Client to client users.
OE.OS	The operating system underlying the MD_Server, the MD_SPS, and the MD_Agent is enhanced by managing it (e.g., patching it due to vulnerabilities) so that it provides secure computing environment. And the OS provides audit storage and timestamp necessary for the TOE's audit records for security relevant events. *Application note: Audit data related to the VPN connection is stored in files and the protection of the audit trail is provided by the OS. In addition to the TOE generates audit records using time source from the OS.* The operating system for the MD_Client is official version provided by mobile device vendors. *Application note: The mobile device for the MD_Client is free from unauthorized modification such as rooting or jailbreaking.*
OE.OP.POLICY	The TOE operation environment is maintained according to the networking environment such as increase/decrease of the hosts or services.
OE.MANAGEMENT.COMM	The web application server (WAS) provided by the operational environment of the TOE provides the environment for authorized administrators (the

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	MD_Server administrator and the MD_Agent administrator) to access TOE through the web browser so that they can perform security management of the TOE. SSL library provided by operational environment of the TOE provides secure communication between web browser on the administrator's PC and TOE when the authorized administrator performs security management of the TOE. The MD_Agent and the mobile device for the MD_Client must be registered to the MD_SPS beforehand to use them for VPN communication, SSL library also provides secure communication between the MD_SPS and TOE components during registration.
OE.CRYPTO	Java cryptographic library and OpenSSL provided by operational environment of the TOE provides cryptographic services for secure TOE operation. Also, private key/public key pairs used by the TOE for registered mobile device and MD_Agent check, and sever authentication are securely generated and managed by IT environment.
OE.DATA.REG	The MD_Agent administrator stores the client user reg. ID/password to the DBMS through the MD_Agent, and

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	securely delivers them to the client user. The MD_Server administrator stores the MD_Agent reg. ID/password to the DBMS through the MD_SPS, and securely delivers them to the MD_Agent administrator.
OE.DBMS	The DBMS provided by operational environment of the TOE stores and maintains TSF data and audit data necessary for the operation of the TOE. The DBMS administrator from the organization that uses the TOE is responsible for secure operation of the DBMS. *Application note: All audit data except for those related to the VPN connection is stored in the DBMS.*
OE.LDAP	The LDAP provided by operational environment of the TOE provides the environment for management of the data necessary for the Mobile-Based VPN policy of the TOE.
OE.NETWORKING.DEVICE	There exist various networking devices to support operation of the TOE according to the various TOE operational environment type of the customer site, and the internal network of the organization is protected by network boundary protection devices such as firewall.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

4.3 Security Objectives Rationale

Security objectives rationale proves that the stated security objectives are appropriate, sufficient to address security problems, not excessive, and necessary.

The rationale for security objectives demonstrates the following.

• Each assumption, threat, and organizational security policy is addressed by at least one of the security objectives.

• Each security objective addresses at least one assumption, threat, or organizational security policy.

[Table 9] Mappings between Security Problem Definition and Security Objectives

Security Objectives / SPD	Security Objectives for the TOE								Security Objectives for the Operational Environment											
	O.AUDIT	O.DATA.PROTECTION	O.ADMIN.I&A	O.CUSER.AUTH	O.VPN.POLICY	O.MANAGEMENT	O.SECURE.STATE	O.TESTING.EXT	OE.PHYSICAL	OE.ADMIN	OE.CUSER	OE.CLIENT.DISTRIBUTION	OE.OS	OE.OP.POLICY	OE.MANAGEMENT.COMM	OE.CRYPTO	OE.DATA.REG	OE.DBMS	OE.LDAP	OE.NETWORKING.DEVICE
T.UNAUTH.ACCESS		●																		
T.ADMIN.DISGUISE			●																	
T.CUSER.DISGUISE				●																
T.REPEAT.AUTH			●																	
T.SW.FAILURE							●													
T.DISABLE.EXT								●												
P.MOBILE.VPN					●															
P.CRYPTO		●																		
P.AUDIT	●												●					●		
P.MANAGEMENT						●														
A.PHYSICAL									●											
A.ADMIN										●										

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Security Objectives / SPD	Security Objectives for the TOE								Security Objectives for the Operational Environment											
	O.AUDIT	O.DATA.PROTECTION	O.ADMIN.I&A	O.CUSER.AUTH	O.VPN.POLICY	O.MANAGEMENT	O.SECURE.STATE	O.TESTING.EXT	OE.PHYSICAL	OE.ADMIN	OE.CUSER	OE.CLIENT.DISTRIBUTION	OE.OS	OE.OP.POLICY	OE.MANAGEMENT.COMM	OE.CRYPTO	OE.DATA.REG	OE.DBMS	OE.LDAP	OE.NETWORKING.DEVICE
A.CUSER											●									
A.CLIENT.DISTRIBUTION												●								
A.OS													●							
A.OP.POLICY														●						
A.MANAGEMENT.COMM															●					
A.CRYPTO																●				
A.DATA.REG																	●			
A.DBMS																		●		
A.LDAP																			●	
A.NETWORKING.DEVICE																				●

4.3.1 Rationale for Security Objectives for the TOE

O.AUDIT

This security objective for the TOE supports the OSP P.AUDIT by ensuring that the TOE records security related events and provides measures to review recorded data, therefore.

O.DATA.PROTECTION

This security objective for the TOE counters the threat T.UNAUTH.ACCESS by ensuring

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

that the TOE provides confidentiality and integrity of user data transmitted between TOE components, and supports the OSP P.CRYPTO by ensuring that the TOE performs cryptographic key management and operations according to the national or international standard to provide confidentiality and integrity.

O.ADMIN.I&A

This security objective for the TOE counters threats T.ADMIN.DISGUISE and T.REPEAT.AUTH by ensuring that the TOE identifies and authenticates the MD_Agent administrator and the MD_Server administrator as authorized administrators and takes actions for unsuccessful authentication.

O.CUSER.AUTH

This security objective for the TOE counters the threat T.CUSER.DISGUISE by ensuring that the TOE authenticates the client user.

O.VPN.POLICY

This security objective for the TOE supports the OSP P.MOBILE.VPN by ensuring that the TOE controls information flows of user data between TOE components according to the Mobile-Based VPN policy.

O.MANAGEMENT

This security objective for the TOE the OSP P.MANAGEMENT by ensuring that the TOE provides management measures to securely manage the TOE the authorized administrator and the client user.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

O.SECURE.STATE

This security objective for the TOE counters the threat T.SW.FAILURE by ensuring that the TOE maintains secure state in case of software failure such as the TOE's critical process runtime errors

O.TESTING.EXT

This security objective for the TOE counters the threat T.DISABLE.EXT by ensuring that the TOE conducts testing of external entities, necessary for the TSF operation, interacting with the TOE.

4.3.2 Rationale for Security Objective for the Operational Environment

OE.PHYSICAL

This security objective for the operational environment supports the assumption A.PHYSICAL by ensuring that the MD_Server, the MD_SPS, and the MD_Agent are located in a physically secure environment protected from physical access.

OE.ADMIN

This security objective for the operational environment supports the assumption A.ADMIN by ensuring that authorized administrators are non-hostile and properly trained about the TOE management function, and follow all administrator guidance.

OE.CUSER

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

This security objective for the operational environment supports the assumption A.CUSER by ensuring that client users are non-hostile and properly trained about the TOE usage, and don't disclose the authentication data necessary for the TOE usage, and are responsible for physical security of the mobile device with the MD_Client.

OE.CLIENT.DISTRIBUTION

This security objective for the operational environment supports the assumption A.CLIENT.DISTRIBUTION by ensuring that the organization that uses the TOE is responsible for the secure distribution of the MD_Client to client users.

OE.OS

This security objective for the operational environment supports the assumption A.OS by ensuring that the operating system underlying the MD_Server, the MD_SPS, and the MD_Agent is enhanced by managing it (e.g., patching it due to vulnerabilities) so that it provides secure computing environment, and that for the MD_Client is official version provided by mobile device vendors free from unauthorized modification such as rooting or jailbreaking. Also, this supports the assumption A.OS and the OSP P.AUDIT by ensuring that the OS provides audit storage and timestamp necessary for the TOE's audit records for security relevant events.

OE.OP.POLICY

This security objective for the operational environment supports the assumption A.OP.POLICY by ensuring that the TOE operation environment is maintained

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

according to the networking environment such as increase/decrease of the hosts or services.

OE.MANAGEMENT.COMM

This security objective for the operational environment supports the assumption A.MANAGEMENT.COMM by ensuring that the operational environment provides web browser necessary for security management by authorized administrators, and SSL protocols JSSE necessary for protection of TSF data.

OE.CRYPTO

This security objective for the operational environment supports the assumption A.CRYPTO by ensuring that Java cryptographic library JCE and OpenSSL provided by operational environment of the TOE provides cryptographic services for secure TOE operation, and private key/public key pairs used by the TOE for registered mobile device and MD_Agent check, and sever authentication are securely generated and managed by IT environment.

OE.DATA.REG

This security objective for the operational environment supports the assumption A.DATA.REG by ensuring that authorized administrators manage information necessary for registration of the MD_Client and the MD_Agent securely.

OE.DBMS

This security objective for the operational environment supports the assumption

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

A.DBMS by ensuring that the DBMS provided by operational environment of the TOE stores and maintains TSF data and audit data necessary for the operation of the TOE, and the DBMS administrator from the organization that uses the TOE is responsible for secure operation of the DBMS.

OE.LDAP

This security objective for the operational environment supports the assumption A.LDAP by ensuring that the LDAP provided by operational environment of the TOE provides the environment for management of the data necessary for the Mobile-Based VPN policy of the TOE.

OE.NETWORKING.DEVICE

This security objective for the operational environment supports the assumption A.NETWORKING.DEVICE by ensuring that there exist various networking devices to support operation of the TOE according to the various TOE operational environment type of the customer site, and the internal network of the organization is protected by network boundary protection devices such as firewall.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

5. Extended Components Definition

There are no extended components in this Security Target.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6. Security Requirements

This section describes security functional requirements and security assurance requirements to be satisfied by the TOE.

This Security Target defines all subjects, objects, operations, security attributes, and external entities that are necessary for the TOE operation as follows;

(1) S.CLIENT: a subject that requests VPN connection on behalf of the client user, and has following security attributes;

- SA.MDEVICE_ID: mobile device ID installed with the MD_Client,
- SA.C_ALGO: list of cryptographic algorithm that can be used VPN connection,
- SA.CPUBLIC_KEY1: the MD_Client Reg. public key used to check if a TOE component requesting VPN connection is allowed to do that (for the MD_Server), and
- SA.CPUBLIC_KEY2: the MD_Client Reg. public key used to check if a TOE component requesting VPN connection is allowed to do that (for the MD_Agent).

(2) S.SERVER: a subject that receives VPN connection on behalf of the MD_Server, and has following security attributes;

- SA.SERVER_IP: IP address of the server installed with the MD_Server,
- SA.SERVER_PORT: port number of the server installed with the MD_Server,
- SA.S_ALGO: list of cryptographic algorithm that can be used VPN connection, and
- SA.SPUBLIC_KEY1: the MD_Server public key for server authentication.

(3) S.AGENT: a subject that requests and receives VPN connection on behalf of the MD_Agent, and has following security attributes;

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

- SA.AGENT_ID: the MD_Agent Reg. ID,
- SA.AGENT_IP: IP address of the host installed with the MD_Agent.
- SA.AGENT_PORT: port number of the host installed with the MD_Agent,
- SA.A_ALGO: list of cryptographic algorithm that can be used VPN connection,
- SA.APUBLIC_KEY1: the MD_Agent public key for server authentication, and
- SA.APUBLIC_KEY2: the MD_Agent Reg. public key used to check if a TOE component requesting VPN connection is allowed to do that (for the MD_Server).

(4) I.PACKET: data transmitted from a subject that request VPN connection to a subject that receives that request, and has following security attributes;

- SA.D_IP: destination IP address,
- SA.D_PORT: destination port number,
- SA.S_IP: source IP address, and
- SA.S_PORT: source port number.

(5) Operations

- Generate: generation of MAC of transmitted data after successful establishment of secure channel,
- Verify: verification of MAC of transmitted data after successful establishment of secure channel, verification of fingerprint for server authentication, verification of information related to a TOE component that requests VPN connection,
- Encrypt: encryption of transmitted data after successful establishment of secure channel,
- Decrypt: decryption of transmitted data after successful establishment of secure channel,
- Connect: VPN connection between TOE components, and

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

- Transmit: data transmission between TOE components.

(6) Client user: a subject that requests VPN connection through the MD_Client and manages the MD_Client.

(7) MD_Agent administrator: a subject that manages the MD_Agent.

(8) MD_Server administrator: a subject that manages the MD_Server.

(9) External entities necessary for the TOE operation;

- Web browser, WAS, and SSL library: environment for the MD_Server administrator and the MD_Agent administrator for security management,
- JCE library: environment for encryption and decryption of data such as configuration parameters and license files for the TOE operation, private/public key pair generation,
- OpenSSL: private/public key pair generation (for iOS),
- LDAP: environment for management of information related to TOE components and session data for VPN connection, and
- DBMS: environment for storage of TSF data and audit data of the TOE.

6.1 Security Functional Requirements

In this section of the Security Target defines security functional requirement derived from CC Part 2 in order to meet security objectives described in the Chapter 4.

The following table summarizes the security functional components used in this Security Target.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

[Table 10] Security Functional Requirements

Security Functional Class	Security Functional Component	
Security audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User data protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITT.1	Basic internal transfer protection
Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition – MD_Agent administrator
	FIA_ATD.1(2)	User attribute definition – MD_Server administrator
	FIA_SOS.1	Authentication of secrets
	FIA_UAU.2(1)	User authentication before any action – client user
	FIA_UAU.2(2)	User authentication before any action – MD_Agent administrator
	FIA_UAU.2(3)	User authentication before any action – MD_Server administrator
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	User identification before any action - MD_Agent administrator
	FIA_UID.2(2)	User identification before any action - MD_Server administrator
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	Management of TSF data
	FMT_SMF.1	Specification of Management Functions

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_TEE.1	Testing of external entities
Resource utilisation	FRU_FLT.1	Degraded fault tolerance
TOE access	FTA_SSL.3(1)	TSF-initiated termination – client user
	FTA_SSL.3(2)	TSF-initiated termination – authorized administrator

The following table shows the relationships between the security functional components and the TOE components in the Security Target.

[Table 11] Relationship between SFRs and TOE components

SFR	MD_Client[8]	MD_Server	MD_SPS	MD_Agent
FAU_GEN.1		●	●	●
FAU_SAR.1		●	●	●
FCS_CKM.1	●	●		●
FCS_CKM.2	●	●		●
FCS_CKM.4	●	●		●
FCS_COP.1	●	●		●
FDP_IFC.1	●	●		●
FDP_IFF.1	●	●		●
FDP_ITT.1	●	●		●
FIA_AFL.1			●	●
FIA_ATD.1(1)				●
FIA_ATD.1(2)			●	
FIA_SOS.1	●		●	●
FIA_UAU.2(1)	●			

[8] The MD_Client library meets SFRs for the MD_Client except for those from FIA class and FMT_MTD.1 for client user authentication data management.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

SFR	MD_Client[8]	MD_Server	MD_SPS	MD_Agent
FIA_UAU.2(2)				●
FIA_UAU.2(3)			●	
FIA_UAU.7	●		●	●
FIA_UID.2(1)				●
FIA_UID.2(2)			●	
FMT_MOF.1	●	●	●	●
FMT_MSA.1				●
FMT_MSA.3			●	●
FMT_MTD.1	●	●	●	●
FMT_SMF.1	●	●	●	●
FMT_SMR.1	●	●	●	●
FPT_FLS.1		●		●
FPT_TEE.1		●	●	●
FRU_FLT.1		●		●
FTA_SSL.3(1)	●			
FTA_SSL.3(2)			●	●

6.1.1 Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shut-down of audit function;

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

c) ["Auditable Events" of [Table 12]]

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, ["Additional Audit Record" of [Table 12]].

[Table 12] Auditable Events

SFR	Auditable Event	Additional Audit Record
FDP_IFF.1	Information flow request and acknowledgement using VPN	Comparison result of cipher suite Verification result of MD_Client Reg. public key
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions	IP address of administrator's PC
FIA_UAU.2(2) FIA_UAU.2(3) FIA_UID.2(1) FIA_UID.2(2)	Success and failure of identification and authentication	IP address of administrator's PC
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF by administrator	IP address of administrator's PC
FMT_MSA.1	All modifications of the values of security attributes by administrator	IP address of administrator's PC
FMT_MTD.1	All modifications to the values of TSF data by administrator	IP address of administrator's PC
FTA_SSL.3(1)	Termination of an interactive VPN session of the client user by the TSF	-

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FTA_SSL.3(2)	Termination of an interactive administrator's session by the TSF	-

Application note: Audit records of auditable events from FDP_IFF.1 and FTA_SSL.3(1) are stored in a file in the MD_Server and the MD_Agent, whereas audit records of the other events are stored in the DBMS which is operational environment of the MD_SPS and the MD_Agent. Auditable events from FDP_IFF.1 and FTA_SSL.3(1) are stored in the file of the MD_Server and the MD_Agent.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [the following authorized administrators] with the capability to read [the following audit data] from the audit records.

Authorized Administrator	**Audit Data**
MD_Server administrator	Audit data generated by the MD_Server Audit data generated by the MD_SPS
MD_Agent administrator	Audit data generated by the MD_Agent

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.2 Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman key exchange method] and specified cryptographic key sizes [1024bits, 2048bits] that meet the following: [RFC 4253 The Secure Shell (SSH) Transport Layer Protocol].

Application note: This SFR is defined to generate session keys for TOE cryptographic operations after establishment of secure channel, and the resulting cryptographic keys are as follows:

Cryptographic Algorithm	Cryptographic Key Sizes
ARIA	128/192/256bits
SEED	128bits
HMAC-SHA-1	160bits

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [Diffie-Hellman key exchange method] that meets the following: [Diffie-Hellman key exchange method].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [physical destruction by overwriting memory data with '0'] that meets the following: [none].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [cryptographic operations listed in the table below] in accordance with a specified cryptographic algorithm [cryptographic algorithms listed in

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

the table below] and cryptographic key sizes [cryptographic key sizes listed in the table below] that meet the following: [standards listed in the table below].

Standard	Cryptographic Algorithm	Cryptographic Key Size	Cryptographic Operation
KSX 1213:2004	ARIA	128/192/256bits	using CBC-mode, encryption and decryption of transmitted user data during VPN communication
TTAS.KO-12.004	SEED	128bits	using CBC-mode, encryption and decryption of transmitted user data during VPN communication
NIST FIPS PUB 180-2	SHA-1	none	Hashing
NIST FIPS PUB 198	HMAC-SHA-1	160bits	HMAC for message authentication

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.3 User data protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Mobile-Based VPN policy] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

[

a) List of subjects;

- S.CLIENT: a subject that requests VPN connection on behalf of the client user,
- S.SERVER: a subject that receives VPN connection on behalf of the MD_Server, and
- S.AGENT: a subject that requests and receives VPN connection on behalf of the MD_Agent.

b) List of information

- I.PACKET: data transmitted from a subject that request VPN connection to a subject that receives that request.

c) List of operations

- Generate: generation of MAC of transmitted data after successful establishment of secure channel,
- Verify: verification of MAC of transmitted data after successful establishment of secure channel, verification of fingerprint for server authentication, verification of information related to a TOE component that requests VPN

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

connection,

- Encrypt: encryption of transmitted data after successful establishment of secure channel,
- Decrypt: decryption of transmitted data after successful establishment of secure channel,
- Connect: VPN connection between TOE components, and
- Transmit: data transmission between TOE components.

]

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [Mobile-Based VPN policy] based on the following types of subject and information security attributes: [the following list of subjects and information controlled under the SFP, and for each the security attributes].

[

a) List of subjects and security attributes

Subject	Security attribute
S.CLIENT	SA.MDEVICE_ID: mobile device ID installed with the MD_Client, SA.C_ALGO: list of cryptographic algorithm that can be used VPN connection, SA.CPUBLIC_KEY1: the MD_Client Reg. public key used to check

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	if a TOE component requesting VPN connection is allowed to do that (for the MD_Server), and SA.CPUBLIC_KEY2: the MD_Client Reg. public key used to check if a TOE component requesting VPN connection is allowed to do that (for the MD_Agent).
S.SERVER	SA.SERVER_IP: IP address of the server installed with the MD_Server, SA.SERVER_PORT: port number of the server installed with the MD_Server, SA.S_ALGO: list of cryptographic algorithm that can be used VPN connection, and SA.SPUBLIC_KEY1: the MD_Server public key for server authentication.
S.AGENT	SA.AGENT_ID: the MD_Agent Reg. ID, SA.AGENT_IP: IP address of the host installed with the MD_Agent. SA.AGENT_PORT: port number of the host installed with the MD_Agent, SA.A_ALGO: list of cryptographic algorithm that can be used VPN connection, SA.APUBLIC_KEY1: the MD_Agent public key for server authentication, and SA.APUBLIC_KEY2: the MD_Agent Reg. public key used to check

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

	if a TOE component requesting VPN connection is allowed to do that (for the MD_Server).

b) List of information and security attributes

Information	Security attribute
I.PACKET	SA.D_IP: destination IP address, SA.D_PORT: destination port number, SA.S_IP: source IP address, and SA.S_PORT: source port number.

].

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:

[

(1) 1st tunneling

a) S.AGENT is allowed to connect VPN connection to S.SERVER if the following rules hold;

- SA.D_IP and SA.D_PORT of I.PACKET are identical to SA.SERVER_IP and SA.SERVER_PORT of S.SERVER.
- SA.A_ALGO of S.AGENT is included in SA.S_ALGO of S.SERVER, and secure channel is established after successful key exchange.
- S.SERVER verifies SA.AGENT_ID and SA.APUBLIC_KEY2 of S.AGENT have been registered.

b) S.AGENT is allowed to transmit information necessary for 3rd tunneling to S.SERVER using established secure channel.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

(2) 2nd tunneling

a) S.CLIENT is allowed to connect VPN connection to S.SERVER if the following rules hold;

- SA.D_IP and SA.D_PORT of I.PACKET are identical to SA.SERVER_IP and SA.SERVER_PORT of S.SERVER.
- SA.A_ALGO of S.CLIENT is included in SA.S_ALGO of S.SERVER, and secure channel is established after successful verification of SA.SPUBLIC_KEY1 fingerprint for server authentication and key exchange.
- S.SERVER verifies SA.MDEVICE_ID and SA.CPUBLIC_KEY1 of S.CLIENT have been registered.

b) S.SERVER is allowed to transmit information necessary for 3rd tunneling to S.CLIENT using established secure channel.

(3) 3rd tunneling

a) S.CLIENT is allowed to connect VPN connection to S.AGENT if the following rules hold;

- In the environment with S.SERVER,
  - SA.D_IP and SA.D_PORT of I.PACKET transmitted by S.CLIENT are identical to SA.SERVER_IP and SA.SERVER_PORT of S.SERVER, and SA.D_IP and SA.D_PORT of I.PACKET remote port-forwarded to S.AGENT by S.SERVER are identical to SA.AGENT_IP 및 SA.AGENT_PORT of S.AGENT.
  - SA.A_ALGO of S.CLIENT is included in SA.S_ALGO of S.CLIENT, and secure channel is established after successful key exchange.

Application note: In the environment with S.SERVER, S.SERVER plays a

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

role as relay server between S.CLIENT and S.AGENT.

- In the environment without S.SERVER,
  - SA.D_IP and SA.D_PORT of I.PACKET are identical to SA.AGENT_IP and SA.AGENT_PORT of S.AGENT.
  - SA.A_ALGO of S.CLIENT is included in SA.S_ALGO of S.CLIENT, and secure channel is established after successful verification of SA.APUBLIC_KEY1 fingerprint for server authentication and key exchange.
- S.AGENT verifies SA.MDEVICE_ID and SA.CPUBLIC_KEY2 of S.CLIENT have been registered.

b) S.AGENT is allowed to transmit information related to internal network service channel to S.CLIENT using established secure channel.

(4) After VPN connection is allowed, transmitting subject encrypts and generates MAC of I.PACKET, receiving subject decrypts and verifies MAC of I.PACKET.

].

FDP_IFF.1.3 The TSF shall enforce the [the following rules].

[

(1) S.CLIENT and S.AGENT are allowed to retry to connect VPN connection 3 times at most if automatic reconnection is set.

(2) S.CLIENT is allowed to maintain VPN connection if connection maintenance is set.

(3) The client user of S.CLIENT is allowed to access service channels through the 3rd tunneling if the user permission is 'allowed'.

(4) The client user of S.CLIENT is allowed to access service channels through the 3rd tunneling if the user role permission is 'allowed'.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

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

[

(1) All VPN connections are denied except for those allowed in FDP_IFF.1.2 and FDP_IFF.1.3.

(2) The client user of S.CLIENT is denied to access service channels through the 3rd tunneling if the user permission is 'denied'.

(3) The client user of S.CLIENT is denied to access service channels through the 3rd tunneling if the user role permission is 'denied'.

(4) S.CLIENT terminates VPN connection after 280 seconds ~ 300 seconds of the client user inactivity if connection maintenance is not set.

].

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ITT.1.1 TSF shall enforce the [Mobile-Based VPN policy] to prevent the *disclosure, modification* of user data when it is transmitted between physically-separated parts of the TOE.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.4 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 *[3]* unsuccessful authentication attempts occur related to [consecutive authentication of authorized administrators (the MD_Agent administrator and the MD_Server administrator)].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [lock the account for 10 minutes to prevent further authentication].

FIA_ATD.1(1) User attribute definition – MD_Agent administrator

Hierarchical to: No other components.

Dependencies: No dependencies.

The TSF shall maintain the following list of security attributes belonging to individual **MD_Agent administrator:** [IP address of the MD_Agent administrator's PC].

FIA_ATD.1(2) User attribute definition – MD_Server administrator

Hierarchical to: No other components.

Dependencies: No dependencies.

The TSF shall maintain the following list of security attributes belonging to individual **MD_Server administrator:** [IP address of the MD_Server administrator's PC].

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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 following metric].

[

- Length: minimum 8 ~ 30 characters
- Combination rule
  - Combination of alphabets (26 characters), numbers (10 digits), special characters
  - Must include at least one alphabet and one number
- Restrictions
  - Password cannot be same as the ID
  - Same characters or numbers cannot be used consecutively

]

FIA_UAU.2(1) User authentication before any action – client user

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FIA_UAU.2(2) User authentication before any action – MD_Agent administrator

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.2(2) User authentication before any action – MD_Server administrator

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

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 ['●', and authentication failure messages in case of authentication failure] to the **client users** and **authorized administrators** while the authentication is in progress.

Application note: Authentication failure messages are provided for only authorized administrator's authentication.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FIA_UID.2(1) User identification before any action – MD_Agent administrator

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

FIA_UID.2(2) User identification before any action – MD_Server administrator

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.5 Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable* the functions [listed in the table below] to [authorized roles in the table below].

List of Functions	Selected Operation		Authorized Roles
	Disable	Enable	
MD_Server	○	○	MD_Server administrator
MD_SPS	○	○	
MD_Agent	○	○	MD_Agent administrator
Automatic reconnection	○	○	
MD_Agent registration		○	
MD_Client	○	○	Client user
Connection maintenance	○	○	
Automatic reconnection	○	○	
Mobile device registration		○	

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_SMR.1 Security roles

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [Mobile-Based VPN policy] to restrict the ability to *query, modify, delete, [add]* the security attributes [listed in the table below] to [authorized roles in the table below].

List of Security Attributes	Selected Operation				Authorized Role
	Query	Modify	Delete	[Add]	
MD_Agent IP	○	○	○	○	MD_Agent administrator
MD_Agent port	○	○	○	○	
Mobile device ID	○				
MD_Server IP	○	○	○	○	MD_Server administrator
MD_Server Port	○	○	○	○	
MD_Agent ID	○	○	○	○	

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 [Mobile-Based VPN policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorized administrators (the MD_Agent administrator and the MD_Server 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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, query, modify, delete, [add]* the [TSF data listed in the table below] to [authorized roles in the table below].

List of TSF Data	Selected Operation					Authorized Roles
	Change _default	Query	Modify	Delete	[Add]	
Account data for client user Reg.		○	○	○	○	MD_Agent administrator
Client user role		○		○	○	
Connected client user information		○				
MD_Agent configuration parameters	○	○	○	○	○	
MD_Agent VPN connection configuration parameters	○	○	○			
Service channel data		○	○	○	○	
Account data for the MD_Agent administrator		○	○			
Client user authentication data			○		○	Client user
Registration status data		○				

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

MD_Server configuration parameters and management data		○	○	○	○	MD_Server administrator
MD_Server VPN connection configuration parameters	○	○	○			
MD_Agent management information		○	○	○	○	
MD_Client information		○				
Account data for the MD_Server administrator		○	○	○	○	

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependency: No dependencies

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

[

(1) MD_Client security management

a) Enabling/disabling of the MD_Client

b) Management of the MD_Client VPN connection configuration parameters

c) Management of client user authentication data

d) Mobile device registration and registration status query

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

(2) MD_Agent security management

a) Enabling/disabling of the MD_Agent

b) Management of the MD_Agent VPN connection configuration parameters

c) Management of the Mobile-Based VPN policy rules

d) The MD_Agent registration

e) Management of the client user account and role

f) Connected client user information query

g) Management of the MD_Agent configuration parameters

a) Management of service channel data

b) Management of the MD_Agent administrator account

(3) MD_Server and MD_SPS security management

a) Enabling/disabling of the MD_Server and the MD_SPS

b) Management of the MD_Server VPN connection configuration parameters

c) Management of the Mobile-Based VPN policy rules

d) Management of the MD_Server configuration parameters

e) Management of the MD_Agent information

f) Management of the MD_Client information

g) Management of the MD_Server administrator account

].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FMT_SMR.1.1 The TSF shall maintain the roles [client user and authorized administrator (the MD_Agent administrator and the MD_Server administrator)].

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.6 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependency: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [software failures abnormally terminating TOE's critical processes].

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components.

Dependency: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests *[at the request to use external entities (WAS, LDAP, and DBMS) by the MD_Server, the MD_SPS, and the MD_Agent]* to check the fulfillment of [availability of external entities (WAS, LDAP, and DBMS) necessary for the MD_Server, the MD_SPS, and the MD_Agent].

FPT_TEE.1.2 If the test fails, the TSF shall [provide warning messages so that authorized administrator can recover].

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.7 Resource utilisation

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

Dependency: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 The TSF shall ensure the operation of [the Mobile-Based VPN function] when the following failures occur: [software failures abnormally terminating TOE's critical processes].

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.1.8 TOE access

FTA_SSL.3(1) TSF-initiated termination – client user

Hierarchical to: No other components.

Dependency: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive **the MD_Client VPN communication session** after a [280 seconds ~ 300 seconds of client user inactivity when connection maintenance is not set for the MD_Client].

FTA_SSL.3(2) TSF-initiated termination – authorized administrator

Hierarchical to: No other components.

Dependency: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive **administrator** session after a [10 minutes of authorized administrator (the MD_Agent administrator and the MD_Server administrator) inactivity].

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.2 Security Assurance Requirements

In this section of the Security Target defines security assurance requirement derived from EAL3 of CC Part 3.

[Table 13] Security Assurance Requirements

Security Assurance Class	Security Assurance Component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architecture design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedure
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
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.2	Vulnerability analysis

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.2.1 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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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:

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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 Extended components 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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.2.2 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:

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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

ADV_FSP.3 Functional specification with complete summary

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from SFR-enforcing actions and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.2 Architectural design

Dependencies: ADV_FSP.3 Functional specification with complete summary

Developer action elements:

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D 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.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

ADV_TDS.2.5C The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

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

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependency: ADV_FSP.1 Basic Functional Specification

Developer action elements

AGD_OPE.1.1D The developer must provide manual for user operation.

Content and presentation elements

AGD_OPE.1.1C Manual for user operation must include adequate warning for user-approachable functions and privileges that must be restricted to safe environments.

AGD_OPE.1.2C Manual for user operation must state usage methods of interface that are safely provided by TOE for each user role.

AGD_OPE.1.3C Manual for user operation must state usable functions and interface for each user role. Especially, safe values must be adequately expressed for all security parameters under user supervision.

AGD_OPE.1.4C Manual for user operation must clearly give each type for approachable functions that must be performed and related security-related event for each user role.

AGD_OPE.1.5C Manual for user operation must identify all performable operation modes of TOE (operation after error, or operation after errors in operation), their influences and related features.

AGD_OPE.1.6C Manual for user operation must state security solutions that must be satisfied in order to satisfy Security Objective for operational environment as stated in the Security Target according to each user role.

AGD_OPE.1.7C Manual for user operation must be clear and logical.

Evaluator action elements

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

AGD_OPE.1.1E The evaluator must authenticate whether the provided information satisfies 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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.2.4 Life-cycle Support

ALC_CMC.3 Authorisation controls

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.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.3.1C The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Evaluator action elements:

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

ALC_CMS.3 Implementation representation CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.3.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.3.1E 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

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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 Testing: basic design

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:

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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 Functional testing

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:

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

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 authenticate 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.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.2.6 Vulnerability assessment

AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E 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 Basic attack potential.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.3 Security Requirements Rationale

The security requirements must satisfy the security objectives, and as a result, verify that it is appropriate for dealing with security problems.

6.3.1 Security Functional Requirements Rationale

The security requirements rationale shall authenticate the following:

• Each security objective for the TOE is addresses by at least one TOE security functional requirement.

• Each TOE security functional requirement covers at least one security objective for the TOE.

[Table 14] Mappings between Security Objectives for the TOE and TOE SFRs

Security Objective / SFR	Security Objectives for the TOE							
	O.AUDIT	O.DATA.PROTECTION	O.ADMIN.I&A	O.CUSER.AUTH	O.VPN.POLICY	O.MANAGEMENT	O.SECURE.STATE	O.TESTING.EXT
FAU_GEN.1	●							
FAU_SAR.1	●							
FCS_CKM.1		●						
FCS_CKM.2		●						
FCS_CKM.4		●						
FCS_COP.1		●						
FDP_IFC.1					●			
FDP_IFF.1					●			

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

Security Objective / SFR	Security Objectives for the TOE							
	O.AUDIT	O.DATA.PROTECTION	O.ADMIN.I&A	O.CUSER.AUTH	O.VPN.POLICY	O.MANAGEMENT	O.SECURE.STATE	O.TESTING.EXT
FDP_ITT.1		●			●			
FIA_AFL.1			●					
FIA_ATD.1(1)			●					
FIA_ATD.1(2)			●					
FIA_SOS.1			●	●				
FIA_UAU.2(1)				●				
FIA_UAU.2(2)			●					
FIA_UAU.2(3)			●					
FIA_UAU.7			●	●				
FIA_UID.2(1)			●					
FIA_UID.2(2)			●					
FMT_MOF.1						●		
FMT_MSA.1						●		
FMT_MSA.3					●	●		
FMT_MTD.1						●		
FMT_SMF.1						●		
FMT_SMR.1						●		
FPT_FLS.1							●	
FPT_TEE.1								●
FRU_FLT.1							●	
FTA_SSL.3(1)					●			
FTA_SSL.3(2)						●		

FAU_GEN.1 Audit data generation

This component satisfies the security objective for the TOE O.AUDIT by ensuring the ability to define auditable events and generate audit records.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FAU_SAR.1 Audit review

This component satisfies the security objective for the TOE O.AUDIT by ensuring the ability to review audit records by authorized administrators.

FCS_CKM.1 Cryptographic key generation

This component satisfies the security objective for the TOE O.DATA.PROTECTION by ensuring the ability to generate cryptographic keys according to the specified cryptographic key generation algorithm and the specified cryptographic key sizes.

FCS_CKM.2 Cryptographic key distribution

This component satisfies the security objective for the TOE O.DATA.PROTECTION by ensuring the ability to distribute cryptographic keys according to the specified cryptographic key distribution method.

FCS_CKM.4 Cryptographic key destruction

This component satisfies the security objective for the TOE O.DATA.PROTECTION by ensuring the ability to destruct cryptographic keys according to the specified cryptographic key destruction method.

FCS_COP.1 Cryptographic operation

This component satisfies the security objective for the TOE O.DATA.PROTECTION by ensuring the ability to conduct cryptographic operations according to the specified cryptographic operation algorithms and the specified cryptographic key sizes.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FDP_IFC.1 Subset information flow control

This component satisfies the security objective for the TOE O.VPN.POLICY by defining the Mobile-Based VPN policy and ensuring the ability to control information flows between TOE components which request VPN connection

FDP_IFF.1 Simple security attributes

This component satisfies the security objective for the TOE O.VPN.POLICY by providing the Mobile-Based VPN policy rules based on the security attributes.

FDP_ITT.1 Basic internal transfer protection

This component satisfies security objectives for the TOE O.DATA.PROTECTION and O.VPN.POLICY by protecting user data transmitted between physically separated TOE parts from disclosure and modification according to the Mobile-Based VPN policy.

FIA_AFL.1 Authentication failure handling

This component satisfies the security objective for the TOE O.ADMIN.I&A by ensuring the ability to define number of unsuccessful administrator's authentication attempts and take actions when the defined number of unsuccessful authentication attempts has been met.

FIA_ATD.1(1) User attribute definition – MD_Agent administrator

This component satisfies the security objective for the TOE O.ADMIN.I&A by defining list of additional security attributes to identify and authenticate the MD_Agent administrator.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FIA_ATD.1(2) User attribute definition – MD_Server administrator

This component satisfies the security objective for the TOE O.ADMIN.I&A by defining list of additional security attributes to identify and authenticate the MD_Server administrator.

FIA_SOS.1 Verification of secrets

This component satisfies security objectives for the TOE O.ADMIN.I&A and O.CUSER.AUTH by providing mechanism to verify that secrets meet defined quality metrics.

FIA_UAU.2(1) User authentication before any action – client user

This component satisfies the security objective for the TOE O.CUSER.AUTH by ensuring the ability to authenticate authorized client user successfully.

FIA_UAU.2(2) User authentication before any action – MD_Agent administrator

This component satisfies the security objective for the TOE O.ADMIN.I&A by ensuring the ability to authenticate authorized MD_Agent administrator successfully.

FIA_UAU.2(2) User authentication before any action – MD_Server administrator

This component satisfies the security objective for the TOE O.ADMIN.I&A by ensuring the ability to authenticate authorized MD_Server administrator successfully.

FIA_UAU.7 Protected authentication feedback

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

This component satisfies security objectives for the TOE O.ADMIN.I&A and O.CUSER.AUTH by ensuring that only specified feedback information is provided to the user during the authentication.

FIA_UID.2(1) User identification before any action – MD_Agent administrator

This component satisfies the security objective for the TOE O.ADMIN.I&A by ensuring the ability to identify MD_Agent administrator successfully.

FIA_UID.2(2) User identification before any action – MD_Server administrator

This component satisfies the security objective for the TOE O.ADMIN.I&A by ensuring the ability to identify MD_Server administrator successfully.

FMT_MOF.1 Management of security functions behaviour

This component satisfies the security objective for the TOE O.MANAGEMENT by ensuring the ability to manage security features by client user and authorized administrators.

FMT_MSA.1 Management of security attributes

This component satisfies the security objective for the TOE O.MANAGEMENT by ensuring the ability to manage security attributes used for the Mobile-Based VPN policy by authorized administrators.

FMT_MSA.3 Static attribute initialisation

This component satisfies security objectives for the TOE O.MANAGEMENT and O.VPN.POLICY by providing authorized administrator roles to specify alternative initial

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

values to override the default values of security attributes used for the Mobile-Based VPN policy.

FMT_MTD.1 Management of TSF data

This component satisfies the security objective for the TOE O.MANAGEMENT by allowing the client user and authorized administrators to manage TSF data.

FMT_SMF.1 Specification of management functions

This component satisfies the security objective for the TOE O.MANAGEMENT by ensuring the ability to specify management functions related to security attributes, TSF data, security functions.

FMT_SMR.1 Security roles

This component satisfies the security objective for the TOE O.MANAGEMENT by ensuring that users are associated with the client user and authorized administrators role.

FPT_FLS.1 Failure with preservation of secure state

This component satisfies the security objective for the TOE O.SECURE.STATE by ensuring that TSF preserves a secure state when software failures occur.

FPT_TEE.1 Testing of external entities

This component satisfies the security objective for the TOE O.TESTING.EXT by ensuring that TSF runs a suite of tests to check availability of external entities necessary for the accurate TSF operation.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FRU_FLT.1 Degraded fault tolerance

This component satisfies the security objective for the TOE O.SECURE.STATE by ensuring that TSF preserves a secure state when software failures occur.

FTA_SSL.3(1) TSF-initiated termination – client user

This component satisfies the security objective for the TOE O.VPN.POLICY by ensuring termination of interactive VPN communication session after time interval of client user inactivity.

FTA_SSL.3(2) TSF-initiated termination – authorized administrator

This component satisfies the security objective for the TOE O.MANAGEMENT by ensuring termination of interactive administrator's session after time interval of authorized administrator inactivity.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.3.2 Security Assurance Requirements Rationale

The evaluation assurance level of the Security Target is EAL3.

EAL3 - methodically tested and checked, permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behaviour. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential. EAL3 also provides assurance through the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

6.4 Dependency Rationale

6.4.1 Dependency of Security Functional Requirements

The following table shows the dependencies of the security functional requirements.

[Table 15] Dependencies of SFRs

No.	Functional Component	Dependencies	Reference No. [ST]
1	FAU_GEN.1	FPT_STM.1	- (1)
2	FAU_SAR.1	FAU_GEN.1	1
3	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	4, 6 5
4	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	3 5
5	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	3
6	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	3 5
7	FDP_IFC.1	FDP_IFF.1	8
8	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	7 22
9	FDP_ITT.1	[FDP_ACC.1 or FD_IFC.1]	7
10	FIA_AFL.1	FIA_UAU.1	15, 16 (2)
11	FIA_ATD.1(1)	No dependencies	N/A
12	FIA_ATD.1(2)	No dependencies	N/A
13	FIA_SOS.1	No dependencies	N/A
14	FIA_UAU.2(1)	FIA_UID.1	- (3)
15	FIA_UAU.2(2)	FIA_UID.1	18 (4)
16	FIA_UAU.2(3)	FIA_UID.1	19 (4)
17	FIA_UAU.7	FIA_UAU.1	14, 15, 16 (2)
18	FIA_UID.2(1)	No dependencies	N/A

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

19	FIA_UID.2(2)	No dependencies	N/A
20	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	24 25
21	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	7 24 25
22	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	21 25
23	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	24 25
24	FMT_SMF.1	No dependencies	N/A
25	FMT_SMR.1	FIA_UID.1	18, 19 (4)
26	FPT_FLS.1	No dependencies	N/A
27	FPT_TEE.1	No dependencies	N/A
28	FRU_FLT.1	FPT_FLS.1	26
29	FTA_SSL.3(1)	No dependencies	N/A
30	FTA_SSL.3(2)	No dependencies	N/A

(1) FAU_GEN.1 depends upon FPT_STM.1 and this dependency is satisfied by the security objective for the operational environment OE.OS, as the TOE records auditable events using reliable time stamps provided by operating system which is TOE operational environment.

(2) FIA_AFL.1 and FIA_UAU.7 depend upon FIA_UAU.1, and this dependency is satisfied by FIA_UAU.2(1), FIA_UAU.2(2) and FIA_UAU.2(3) which are hierarchical to FIA_UAU.1.

(3) The MD_Client is installed and operated on the only one mobile device which belongs to only one client user, thus the client user identification is unnecessary. Therefore the dependency of FIA_UAU.2(1) upon FIA_UID.1 is unnecessary.

(4) FIA_UAU.2(2), FIA_UAU.2(3) and FMT_SMR.1 depend upon FIA_UID.1, and this dependency is satisfied by FIA_UID.2(1) and FIA_UID.2(2) which are hierarchical to

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

FIA_UID.1.

6.4.2 Dependency of Security Assurance Requirements

All dependencies of each assurance package provided by the CC are already satisfied.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

7. TOE Summary Specification

7.1 Mobile-Based VPN

The TOE enforces the Mobile-Based VPN policy to protect user data from disclosure and modification, which is transmitted between the MD_Agent and the MD_Server (the 1st tunneling), the MD_Client and the MD_Server (the 2nd tunneling), and the MD_Client and the MD_Agent (the 3rd tunneling).

- **The 1st tunneling**

In the environment with the MD_Server, the MD_Agent requests connection through the IP and the port which are used for the MD_Server's VPN communication, and then agrees cryptographic algorithms for VPN communication with the MD_Server. After successful key exchange, session keys are generated and the secure channel is established.

After establishment of the secure channel, the MD_Server checks if the MD_Agent is allowed to connect VPN communication or not by verifying the MD_Agent ID and the MD_Agent Reg. public key.

The MD_Agent transmit information necessary for 3rd tunneling to the MD_Server using established secure channel.

- **The 2nd tunneling**

In the environment with the MD_Server, the MD_Client requests connection through the IP and the port which are used for the MD_Server's VPN communication, and then agrees cryptographic algorithms for VPN communication with the MD_Server. After successful verification of fingerprint for server authentication and key exchange, session keys are generated and the secure channel is established.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

After establishment of the secure channel, the MD_Server checks if the MD_Client is allowed to connect VPN communication or not by verifying the mobile device ID and the MD_Client Reg. public key.

The MD_Server transmits information necessary for 3rd tunneling to the MD_Client using established secure channel.

- **The 3rd tunneling**

The client user can ultimately use service channel provided by internal network using VPN communication through the 3rd tunneling.

In the environment with the MD_Server, the MD_Client requests connection through the IP and the port which are used for the MD_Server's VPN communication, the MD_Server relays communication by conducting remote port-forwarding the request to the port of the MD_Agent which is used for the MD_Agent's VPN communication. The MD_Client agrees cryptographic algorithms for VPN communication with the MD_Agent. After successful key exchange, session keys are generated and the secure channel is established.

In the environment without the MD_Server, the MD_Client directly requests connection through the IP and the port which are used for the MD_Agent's VPN communication. The MD_Client agrees encryption/decryption algorithms, integrity algorithms, and key exchange algorithms for VPN communication with the MD_Agent. After successful verification of fingerprint for server authentication and key exchange, session keys are generated and the secure channel is established.

After establishment of the secure channel, the MD_Agent checks if the MD_Client is allowed to connect VPN communication or not by verifying the mobile device ID and the MD_Client Reg. public key.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

The MD_Agent transmits information related to internal network service channels to the MD_Client using established secure channel.

Also, the MD_Agent can allow or deny the client user to access service channels based on the user permission or user role permission.

The MD_Client and the MD_Agent are allowed to retry to connect VPN connection 3 times at most if automatic reconnection is set. The MD_Client is allowed to maintain VPN connection if connection maintenance is set, and the MD_Client terminates VPN connection after 280 seconds ~ 300 seconds of the client user inactivity if connection maintenance is not set.

After VPN connection is allowed, transmitting TOE component encrypts and generates MAC of transmitted user data, receiving TOE component decrypts and verifies MAC of received user data.

- **Cryptographic services**

The TOE generates cryptographic keys used for encryption/decryption and MAC generation in accordance with Diffie-Hellman key exchange method that meets RFC 4253. Also, the TOE conducts server authentication by verifying fingerprint which is hash value of public key of server side (i.e., the MD_Server or the MD_Agent), which has been stored in the MD_Client during mobile device registration.

Then using generated session keys, the TOE encrypts and decrypts transmitted user data through secure channel using CBC-mode of ARIA or CBC-mode of SEED, and generates and verifies MAC using HMAC-SHA-1.

The TOE uses SHA-1 for key exchange, fingerprint verification for server authentication, and hash value generation for HMAC.

The TOE destroys cryptographic keys by overwriting memory data with '0'.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

7.2 MD_Client

7.2.1 Client user authentication

The TOE authenticates client users using passwords registered by client users themselves after installation of the MD_Client. Passwords entered by client users are protected using '●' character during authentication.

7.2.2 MD_Client security management

The client user enables and disables the MD_Client. The client user can register a mobile device installed with the MD_Client for VPN communication after successful authentication to the MD_Client, set or modify password used for the client user authentication, and configure VPN communication parameters (e.g., connection maintenance and automatic reconnection). Password used for client user authentication must meet the following rules:

- length: minimum 8 ~ 30 characters,
- combination rules:
  - combination of one of alphabet (26 characters), digits (10 characters), and special characters, and,
  - at least both one alphabet character and one digit character included, and
- other rules:
  - password identical to ID is not allowed, and
  - no consecutive, same characters and digits.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

7.3 MD_Server

7.3.1 MD_Server audit data generation

The MD_Server generates log files of events about Mobile-Based VPN connection between the MD_Server itself and other TOE components.

7.3.2 MD_Server security management

The MD_Server administrator can enable and disable the MD_Server after successful identification and authentication to the MD_SPS, and query, modify, delete, and add the MD_Server IP and port, and the MD_Agent ID security attributes which are used for the Mobile-Based VPN policy rules. Also, the MD_Server administrator can query, modify, delete and add the MD_Server configuration parameters and management data, and change default values of, query, and modify the MD_Server VPN connection configuration parameters.

7.3.3 MD_Server testing of external entities

The MD_Server provides testing of external entities whenever it requests to these external entities (LDAP) for services by requesting for the data stored in the LDAP.

7.3.4 MD_Server software failure handling

The MD_Server runs the daemon that checks its own running status (start, stop) regularly

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

(every 5 minutes), and handle software failure by restarting the process which is abnormally terminated.

7.4 MD_SPS

7.4.1 MD_Server administrator identification and authentication

The MD_SPS identifies and authenticates the MD_Server administrator who can conduct security management. The MD_Server administrator accesses to the MD_SPS using web browser (HTTPS), the IP address of the administrator's PC and the entered ID/password are verified against those in the DBMS. Password entered by the MD_Server administrator is protected using '●' character during authentication, and authentication failure messages are occurred in case of authentication failure. When 3 of consecutive unsuccessful authentication attempts have been met, the account is locked for a certain time period (10 minutes) to prevent further authentication.

7.4.2 MD_SPS audit data generation and review

The MD_SPS generates audit data related to auditable event such as the MD_Server administrator authentication (success or failure), 3 unsuccessful authentication attempts, security function management, and TSF data management, and stores audited data through DBMS.

The MD_Server administrator can review the MD_Server and the MD_SPS audit data through the MD_SPS.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

7.4.3 MD_SPS security management

The MD_Server administrator can enable and disable the MD_SPS after successful identification and authentication to the MD_SPS, and query, modify, delete, and add the MD_Agent management information and account data for the MD_Server administrator. Also, the MD_Server administrator can query the MD_Client information. Password used for the MD_Server administrator authentication must meet the following rules:

- length: minimum 8 ~ 30 characters,
- combination rules:
  - combination of one of alphabet (26 characters), digits (10 characters), and special characters, and,
  - at least both one alphabet character and one digit character included, and
- other rules:
  - password identical to ID is not allowed, and
  - no consecutive, same characters and digits.

Also, the TSF terminates the administrator's session when the MD_Server administrator doesn't interact with the MD_SPS for a certain time period (10 minutes).

7.4.4 MD_SPS testing of external entities

The MD_SPS provides testing of external entities (WAS, LDAP, and DBMS) whenever it requests to these external entities for services by calling for web pages to the WAS, requesting for the data stored in the LDAP, and query request to the DBMS.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

7.5 MD_Agent

7.5.1 MD_Agent administrator identification and authentication

The MD_Agent identifies and authenticates the MD_Agent administrator who can conduct security management. The MD_Agent administrator accesses to the MD_Agent using web browser (HTTPS), the IP address of the administrator's PC and the entered ID/password are verified against those in the DBMS. Password entered by the MD_Server administrator is protected using '●' character during authentication, and authentication failure messages are occurred in case of authentication failure. When 3 of consecutive unsuccessful authentication attempts have been met, the account is locked for a certain time period (10 minutes) to prevent further authentication.

7.5.2 MD_Agent audit data generation and review

The MD_Agent generates log files of events about Mobile-Based VPN connection between the MD_Agent itself and other TOE components. Also, the MD_Agent generates audit data related to auditable event such as the MD_Agent administrator authentication (success or failure), 3 unsuccessful authentication attempts, security function management, and TSF data management, and stores audited data through DBMS.

The MD_Agent administrator can review the MD_Agent audit data through the MD_Agent.

7.5.3 MD_Agent security management

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

The MD_Agent administrator can enable and disable the MD_Agent after successful identification and authentication to the MD_Agent, and query, modify, delete, and add the MD_Agent IP and port security attributes which are used for the Mobile-Based VPN policy rules. The MD_Agent administrator can also query mobile device IDs. The MD_Agent administrator can register the MD_Agent, and change default values of, query, modify, delete, and add account data for client user registration, client user role, connected client user information, the MD_Agent configuration parameters, the MD_Agent VPN connection configuration parameters, service channel data, and account data for the MD_Agent administrator. Password used for the MD_Agent administrator authentication must meet the following rules:

- length: minimum 8 ~ 30 characters,
- combination rules:
  - combination of one of alphabet (26 characters), digits (10 characters), and special characters, and,
  - at least both one alphabet character and one digit character included, and
- other rules:
  - password identical to ID is not allowed, and
  - no consecutive, same characters and digits.

Also, the TSF terminates the administrator's session when the MD_Agent administrator doesn't interact with the MD_Agent for a certain time period (10 minutes).

7.5.4 MD_Agent testing of external entities

The MD_Agent provides testing of external entities (WAS, LDAP, and DBMS) whenever it

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved

requests to these external entities for services by calling for web pages to the WAS, requesting for the data stored in the LDAP, and query request to the DBMS.

7.5.5 MD_Agent software failure handling

The MD_Agent runs the daemon that checks its own running status (start, stop) regularly (every 5 minutes), and handle software failure by restarting the process which is abnormally terminated.

Copyright © 2011 Samsung SDS Co., Ltd. All rights reserved