KECS-CR-11-64

Mobiledesk VPN v1.0

Certification Report

Certification No.: KECS-NISS-0356-2011

2011. 12. 29

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2011.12.29	-	Certification report for Mobiledesk VPN v1.0 - First documentation

This document is the certification report for Mobiledesk VPN v1.0 of Samsung SDS.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory Co., Ltd. (KSEL)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL3 evaluation of Mobiledesk VPN v1.0 from Samsung SDS Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is product package which is consisting of software and library provided with corresponding several guidance documents. The TOE provides virtual private network (VPN) functionality to secure communications between mobile devices and the protected network based on the RFCs related to the standard SSH by IETF (Internet Engineering Task Force) [5].

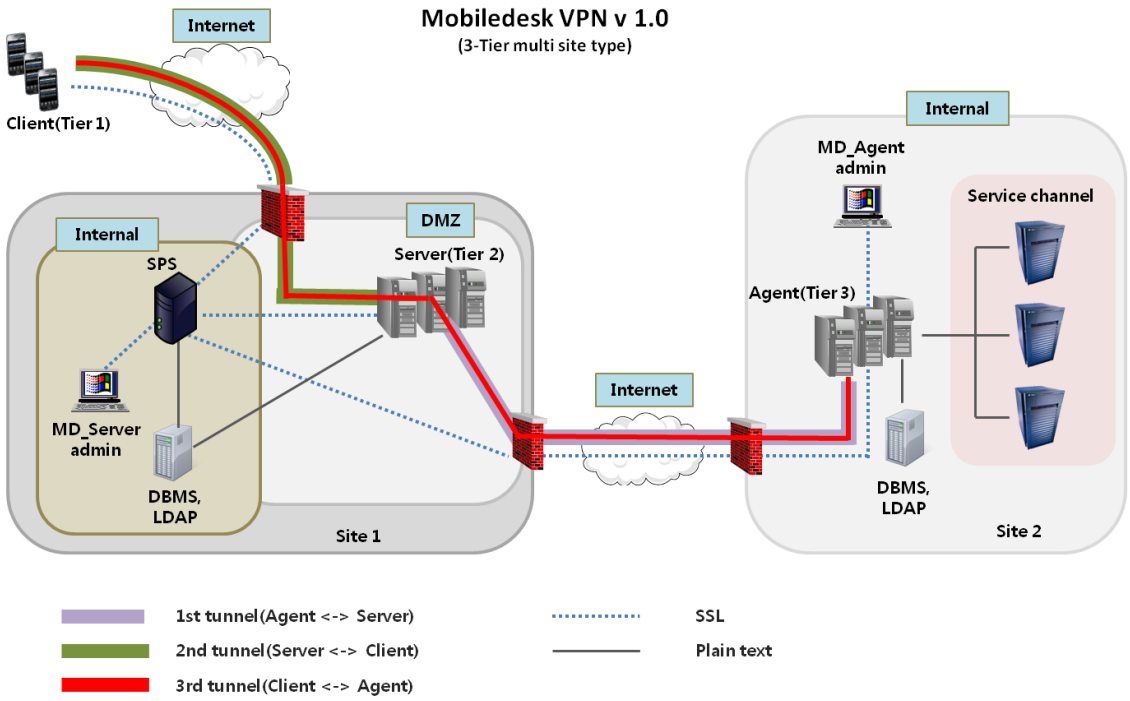
The TOE Mobiledesk VPN v1.0 is composed of the following components:

- 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

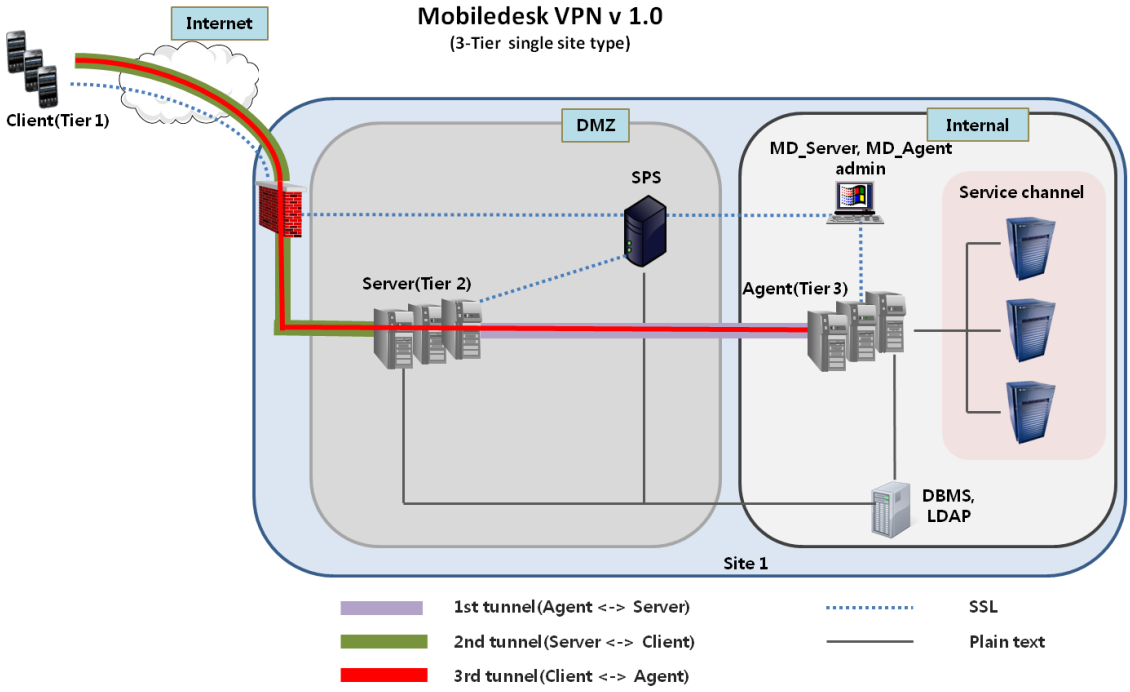
The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory Co., Ltd. (KSEL) and completed on November 30, 2011. This report grounds on the evaluation technical report (ETR) KSEL had submitted [6] and the Security Target (ST) [7].

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL3. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

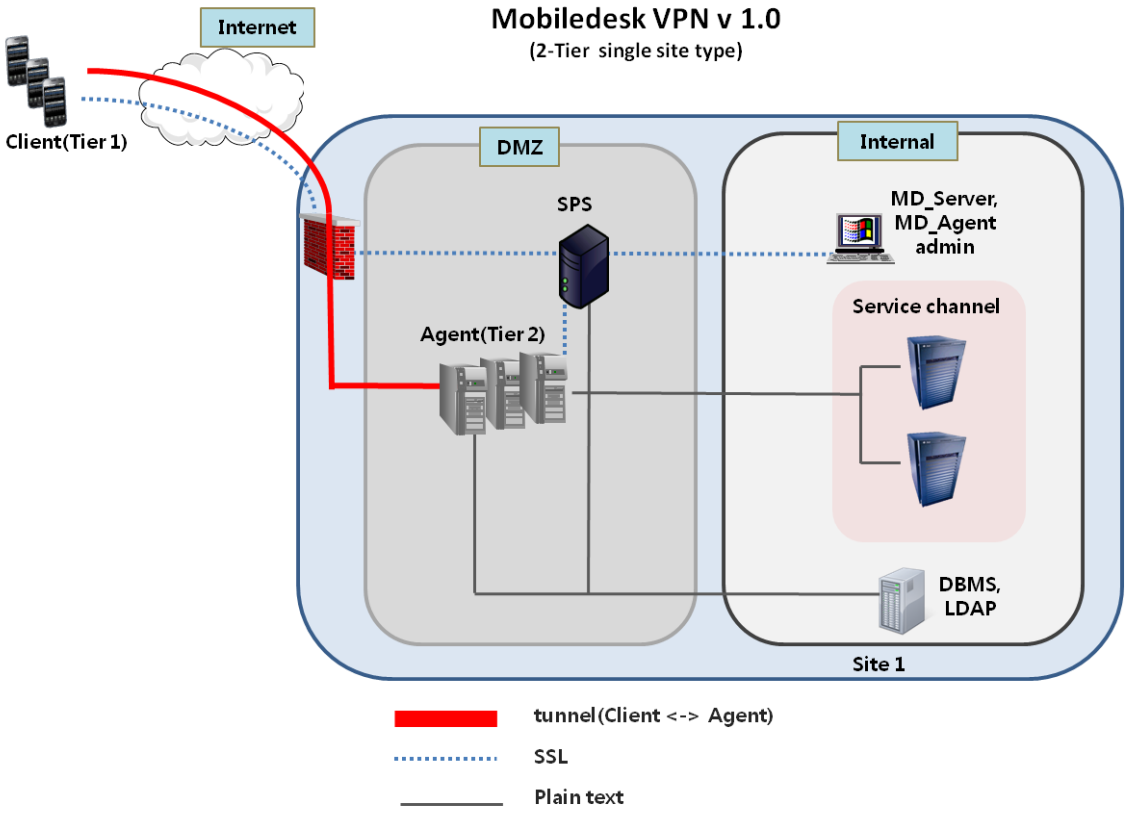
The TOE can be operated in three kinds of networking environments. [Figure 1], [Figure 2], and [Figure 3] show the operational environments of the TOE.



[Figure 1] TOE Operational Environment (Multiple Site Type)



[Figure 2] TOE Operational Environment (3Tier Single Site Type)



[Figure 3] TOE Operational Environment (2Tier Single Site Type)

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

2. Identification

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

Type	Identifier		Release	Delivery Form
SW	MD_Agent	Mobiledesk VPN Agent for Linux Mobiledesk VPN Agent for Windows	v1.0.5 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 Mobiledesk VPN Client Library for iOS	v1.0.4 v1.0.4	Library
DOC	Mobiledesk VPN v1.0 Agent Manual		v1.1	Softcopy
	Mobiledesk VPN v1.0 Server Manual		v1.1	
	Mobiledesk VPN v1.0 Client Manual		v1.1	
	Mobiledesk VPN v1.0 Developer Manual		v1.0	

[Table 1] TOE identification

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009) Korea Evaluation and Certification Regulation for IT Security (July 20, 2011)
TOE	Mobiledesk VPN v1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
EAL	EAL3
Developer	Samsung SDS Co., Ltd.
Sponsor	Samsung SDS Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory Co., Ltd. (KSEL)
Completion Date of Evaluation	November 30, 2011
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [7] by security objectives and security requirements. The TOE provides security features for VPN based on the national or international standard cryptography:

- 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, and
  - The TOE only allows information flows between TOE components that are allowed to use VPN connection,
- 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.

Also, the TOE provides security features to identify and authenticate authorized users, to generate audit records of the auditable events including VPN establishment, and to securely manage the TOE including VPN functionality and authorized user accounts information.

For more details refer to the ST [7].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [7], chapter 3.3):

- The TOE, except for the MD_Client, is located in a physically secure environment of customer's site so that they are protected from physical access.
- Authorized administrators are non-hostile and properly trained about the TOE management function, and follow all administrator guidance. 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.
- The organization that uses the TOE is responsible for the secure distribution of the MD_Client to client users.

- The operating system underlying the TOE, except for the MD_Client, 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. The operating system for the MD_Client is official version provided by mobile device vendors.
- The TOE operation environment is maintained according to the networking environment such as increase/decrease of the hosts or services.
- The operational environment of the TOE provides the secure communication environment for authorized administrators to access the TOE so that they can perform security management of the TOE.
- The operational environment of the TOE provides cryptographic services for secure TOE operation (e.g., private key/public key pairs generation).
- Authorized administrators securely handle data for mobile device and MD_Agent registration.
- 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.
- 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.
- 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.

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

TOE Component	Category	Recommended Specifications
MD_Agent	CPU	Pentium 4 2.6GHz or higher (Quad core or higher)
	OS	Windows Server 2003 (32bit/64bit) Windows Server 2008 (32bit/64bit)

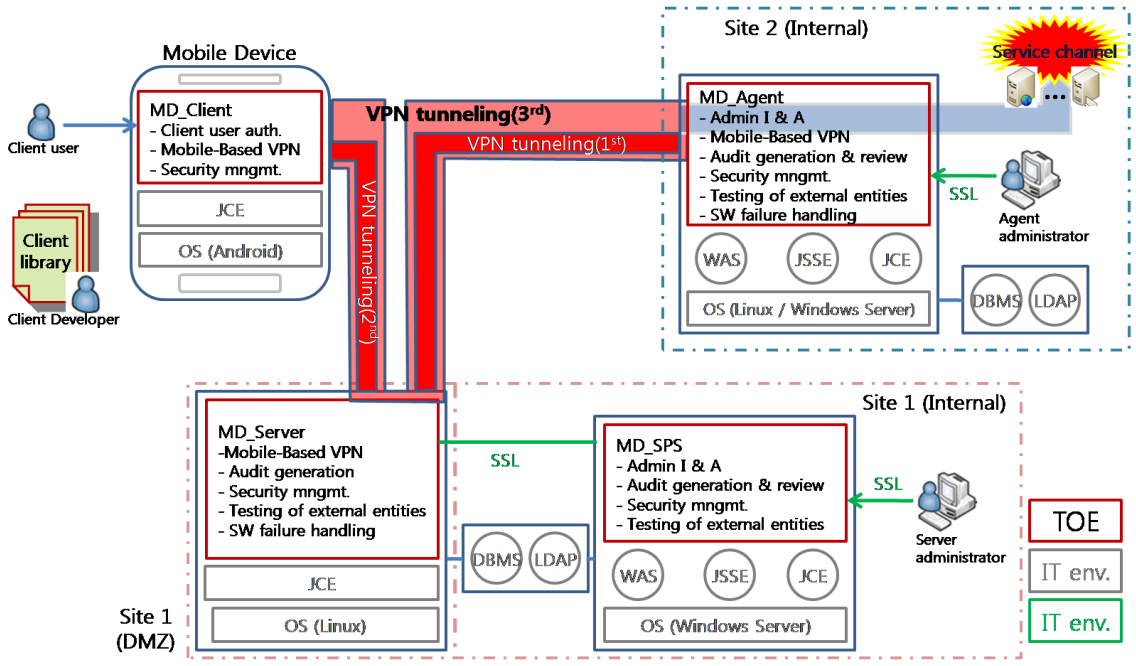
TOE Component		Category	Recommended Specifications
			RedHat Enterprise Linux 5 (Kernel 2.6) (32bit/64bit)
		RAM	4GB or higher
		HDD	30GB or higher
		NIC	One unit of 10/100/1000Mbps
MD_Server		CPU	Pentium 4 2.6GHz or higher (Quad core or higher)
		OS	RedHat Enterprise Linux 5 (Kernel 2.6) (32bit/64bit)
		RAM	4GB or higher
		HDD	64GB or higher
		NIC	One unit of 10/100/1000Mbps
MD_SPS		CPU	Pentium 4 2.6GHz or higher (Quad core or higher)
		OS	Windows Server 2003 (32bit/64bit) Windows Server 2008 (32bit/64bit)
		RAM	4GB or higher
		HDD	30GB or higher
		NIC	One unit of 10/100/1000Mbps
MD_Client	Android	Mobile Device	Samsung, LG, Motorola, HTC
		CPU	ARMv7 720MHz or higher
		OS	Android 2.2, Android 2.3
		RAM	512MB or higher
		Memory	8GB or higher
		Network	3G Network(HSDPA) or Wi-Fi 802.11 b/g/n supported
	iOS	CPU	ARMv7 833Mhz or higher
		OS	iOS 4.3
		RAM	256 MB or higher
		Memory	8GB or higher

TOE Component		Category	Recommended Specifications
		Network	3G Network(HSDPA) or Wi-Fi 802.11 b/g/n supported

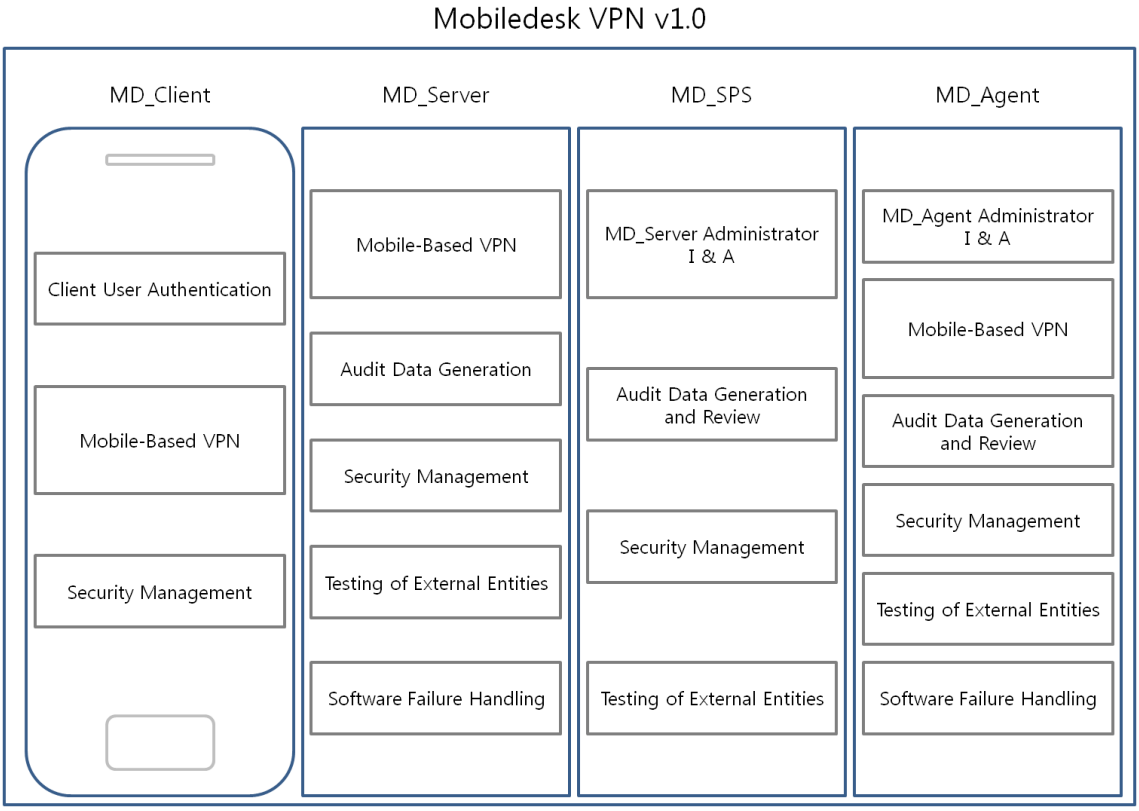
[Table 3] Required non-TOE Hardware and OS

5. Architectural Information

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



[Figure 4] Architectural Information of the TOE



[Figure 5] Logical boundary of the TOE

- The MD_Client is:
  - VPN client application, which is installed and operated on the mobile device by a client user, or
  - VPN client library, which is composed of management features and cryptography libraries needed for a VPN client, and used by a client developer instead of a client user.

  The MD_Client provides security functionality of client user authentication, Mobile-Based VPN client, and security management for itself.

  The MD_Client establishes Mobile-Based VPN through the 2nd and the 3rd tunneling connections in the operational environment with the MD_Server (the relaying server), or the 3rd tunneling connection only in the operational environment without the MD_Server, and then the MD_Client can access service channels in the protected internal network.
- The MD_Agent is VPN gateway server, which is installed and operated in a physically secure place in the organization, ultimately establishes VPN communication with the MD_Client through the 3rd tunneling connection.

The MD_Agent provides security functionality of authorized administrator identification and authentication, Mobile-Based VPN gateway, audit data generation and review, security management for itself, testing of external entities necessary for its operation, and software failure handling.

In the operational environment with the MD_Server which relays VPN communication, the 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_Server is VPN gateway server, which is installed and operated in a physically secure place in the organization, relays VPN tunneling between the Mobiledesk VPN Client and the Mobiledesk VPN Agent using remote port forwarding technique.

  The MD_Server provides security functionality of Mobile-Based VPN gateway, audit data generation, security management for itself, testing of external entities necessary for its operation, and software failure handling.
- The MD_SP is management and authentication server, which is installed and operated together with the MD_Server in a physically secure place in the organization.

  The MD_SPS provides security functionality of authorized administrator identification and authentication, audit data generation and review, security management for itself and the MD_Server, and testing of external entities necessary for its operation.

6. Documentation

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

Identifier	Release	Date
Mobiledesk VPN v1.0 Agent Manual	v1.1	August 3, 2011
Mobiledesk VPN v1.0 Server Manual	v1.1	August 3, 2011
Mobiledesk VPN v1.0 Client Manual	v1.1	August 3, 2011
Mobiledesk VPN v1.0 Developer Manual	v1.0	August 3, 2011

[Table 4] Documentation

7. TOE Testing

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

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

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

Therefore the developer tested all SFRs defined in the ST [7].

The evaluator performed all the developer's tests (a total of 128 tests), and conducted a total of 43 independent testing based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [7]. The evaluator considered followings when devising a test subset:

- TOE security functionality: The TOE provides virtual private network (VPN) functionality between mobile devices and the protected network, and other supporting functionality to manage VPN functionality, and
- Developer's testing evidence: The evaluator analyzed evaluation deliverables for ATE_COV.2, ATE_DPT.1, and ATE_FUN.1 to understand behavior of the TOE security functionality and to select the subset of the interfaces to be tested, and
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL3, and the evaluator tried to balance time and effort of evaluator's activities between EAL3 assurance components.

Also, the evaluator conducted a total of 47 penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, weak cryptography, flaws in networking protocol implementation, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [6].

8. Evaluated Configuration

The TOE is Mobiledesk VPN v1.0. The TOE is product package which is consisting of following components:

- 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

The TOE is identified by each TOE component name and version number including release number. The TOE identification information is provided GUI or CLI according to the TOE component (or both of them).

And the guidance documents listed in this report chapter 6, [Table 4] were evaluated with the TOE.

The TOE can be installed and operated in a three different type of networking environment (i.e., Multiple Site Type, 3Tier Single Site Type, and 2Tier Single Site Type), refer to chapter 1 of this report for details about operational environment of the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [6] which references Single Evaluation Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL3.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The ST doesn't define any extended component. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer uses a CM system that uniquely identifies all configuration items, and the ability to modify these items is properly controlled. Therefore the verdict PASS is assigned to ALC_CMC.3.

The configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is

assigned to ALC_CMS.3.
The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Therefore the verdict PASS is assigned to ALC_DVS.1.
The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.
Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, and the delivery activity.
The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.
The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. It provides a detailed description of the SFR-enforcing subsystems and enough information about the SFR-supporting and SFR-non-interfering subsystems for the evaluator to determine that the SFRs are completely and

accurately implemented. Therefore the verdict PASS is assigned to ADV_TDS.2.
The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, the actions, results and error messages of each TSFI are also described sufficiently that it can be determined whether they are SFR-enforcing, with the SFR-enforcing TSFI being described in more detail than other TSFIs. Therefore the verdict PASS is assigned to ADV_FSP.3.
The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.
Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), and a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

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

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing Basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.2.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing Basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_CMS.3	ALC_CMS.3.1E	PASS	PASS	
	ALC_CMC.3	ALC_CMC.3.1E	PASS	PASS	
	ALC_DVS.1	ALC_DVS.1.1E	PASS	PASS	
		ALC_DVS.1.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.2	ADV_TDS.2.1E	PASS	PASS	PASS
		ADV_TDS.2.2E	PASS	PASS	
	ADV_FSP.3	ADV_FSP.3.1E	PASS	PASS	
		ADV_FSP.3.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.1	ATE_DPT.1.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

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

- The TOE can be configured in a three different ways according to the networking environment, therefore the organization should understand its networking environment and then can select appropriate one.
- The VPN client provided by the developer only supports mobile devices using Android, therefore the organization who want to use mobile devices based on iOS should develop its own VPN client using client library.

- Client users must take proper actions in case of the lost mobile device by informing authorized administrator to prevent to use VPN services provided by the VPN client.
- The mobile device for the VPN client must be free from unauthorized modification such as rooting or jailbreaking.

11. Security Target

The Mobiledesk VPN v1.0 Security Target v1.3, July 5, 2011 [7] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RFC	Request For Comments
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network
Mobile-Based VPN	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.
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.
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 the MD_SPS according to the TOE security policies. It includes the MD_Server administrator and the MD_Agent administrator.

Mobile Device Registration	It refers to the process of storing the mobile device information 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 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.
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.

13. Bibliography

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

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

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

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

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

[5] RFC 4251 The Secure Shell (SSH) Protocol Architecture
RFC 4252 The Secure Shell (SSH) Authentication Protocol
RFC 4253 The Secure Shell (SSH) Transport Layer Protocol

RFC 4254 The Secure Shell (SSH) Connection Protocol
RFC 4256 Generic Message Exchange Authentication for the Secure Shell (SSH)

[6] KSEL-CC-2011-01 Mobiledesk VPN v1.0 Evaluation Technical Report V2.00, November 30, 2011

[7] Mobiledesk VPN v1.0 Security Target v1.3, July 5, 2011