National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Samsung SDS Co, Ltd.

123, Olympic-ro 35-gil, Songpa-gu, Seoul,

Korea 138-240

Samsung SDS Co., LTD Samsung SDS CellWe EMM Suite

Report Number: CCEVS-VR-10618-2015
Dated: May 8, 2015
Version: 0.5

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Kenneth Elliott
Jerry Myers
Ken Stutterheim
Aerospace Corporation
Columbia, MD

Sheldon Durrant
MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

James Arnold
Neal Haley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Samsung SDS Co., LTD CellWe EMM Suite provided by Samsung SDS Co., LTD. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in May 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1.

The Target of Evaluation (TOE) is the is the Samsung SDS Co., LTD Samsung SDS CellWe EMM Suite version 1.1.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the Samsung SDS Co., LTD Samsung SDS CellWe EMM Suite (MDMPP11) Security Target and analysis performed by the evaluation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this

program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Samsung SDS Co., LTD Samsung SDS CellWe EMM Suite version 1.1
Protection Profile	Protection Profile for Mobile Device Management, Version 1.1, 7 March 2014
ST:	Samsung SDS Co., LTD EMM Suite (MDMPP11) Security Target, Version 0.6, May 8, 2015
Evaluation Technical Report	Evaluation Technical Report for Samsung SDS Co., LTD EMM Suite (MDMPP11), Version 1.4, May 8, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Samsung SDS Co., LTD.
Developer	Samsung SDS Co., LTD.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Kenneth Elliott, The Aerospace Corporation
	Jerry Myers, The Aerospace Corporation
	Ken Stutterheim, The Aerospace Corporation

Item	Identifier
	Sheldon Durrant, The MITRE Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The EMM Suite consists of an EMM Server and Agent, where the Server provides centralized management of mobile devices and the Agent software (installed on each device) enforces the policies of the Server on each device

Samsung SDS offers the EMM Server as a software installation for Java 1.7 and Tomcat 7.0 running on Microsoft Windows Server 64-bit operating systems from 2008 R2 through to Windows Server 2012 R2. Once installed, the EMM Server allows administrators to configure policies for devices. Administrators connect securely to the EMM Server using a web browser (whether local to the Server itself or remote) and, through the EMM Server's web interface, can enroll, audit, lock, unlock, manage, and set policies for enrolled mobile devices. The EMM Server includes the RSA Crypto-J 6.1 cryptographic module as part of its software, and the EMM Server's Microsoft Windows platform includes SQL server 2008-2012 and an EJBCA certificate authority.

Samsung SDS provides the EMM Agent software for evaluated Samsung mobile devices (including the Galaxy S4, Note 3, S5, Note 4, and Galaxy Note Edge), and the Agent software, once installed and enrolled with the EMM Server, will apply and enforce administrator configured policies communicated through the EMM to the Agent software.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of collection of server components (MDM server) and mobile device applications (MDM agent).

- EMM Server – Runs on the Java 1.7 and Tomcat 7.0 platforms installed on Microsoft Windows Server 2008 R2 operating system through to Windows Server 2012 R2. The EMM Server also interacts with Microsoft SQL Server 2008 through 2012 and an EJBCA v 4.0.16 certificate authority. While one may deploy the system in several compliant and equivalent configurations, the specific configuration tested during this evaluation consisted of the server running on Windows Server 2012 R2, along with SQL Server 2012 and EJBCA v 4.0.16 certificate authority.
- Agent – The Agent can run on any evaluated Samsung mobile device (including the Galaxy S4, Note 3, S5, Note 4, and Galaxy Note Edge). This evaluation was performed using 32-bit versions of the Android operating system.

3.2 TOE Architecture

The EMM Server actually consists of the following different servers:

1. EMM Server – the main server running to which remote administrators connect. The EMM Server bears responsibility for all logic needed to manage mobile devices.
2. Push Server – the Push Server accepts connections from mobile devices and then relays the messages to and from the EMM Server (for example, to send policies to an agent, or to send back a reply from an agent). One can install multiple Push Servers, in order to allow the overall solution to scale the supported number of mobile devices. Testing was performed using a single Push Server configuration.
3. AppTunnel Server – this server accepts connections from the EMM Client (one of the three portions of the agent software on Android) and allows the Client to upload log files or download mobile applications to be installed by the agent.

The EMM Server allows two types of profiles

An MDM Profile – to control all MDM configurable extensions (for example enforcing password complexity requirements).

EMM Client profile - controls only the configuration of the SDS client app itself (e.g., how a user logs in)

The EMM Agent consists of three different components on evaluated Android platforms:

1. The EMM Client – at the highest level, this provides a UI through which the user may enroll their mobile device. This Client is also responsible for uploading audit logs to the EMM Server and for downloading mobile applications that the Server directs the agent to install.
2. The EMM Agent – this component provides most of the agent's core functionality including the application of policies, reporting policy event triggers to the Server, installation of applications, communication with the Server, among other things. The Agent operates without user intervention and enforces the policies of the Server.
3. The Push Agent – this lowest level component facilitates Push communications with a Push server. It allows both the EMM Agent and other mobile applications to send and receive Push messages.

The EMM Client presents the UI to allow users to start the enrollment process and, once enrolled, to log in and log out.

3.3 Physical Boundaries

The physical boundaries of the EMM Suite are the physical perimeter of the servers hosting the EMM Server and the physical perimeter of the mobile devices being managed by the EMM Server (put another way, the mobile devices running the EMM Agent).

The EMM Server also interacts with Microsoft SQL server and an EJBCA certificate authority.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security Audit
2. Cryptographic support
3. Identification and authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security Audit

The EMM Server can generate and store audit records for security-relevant events as they occur. These events are stored and protected by the EMM Server and can be reviewed by an authorized Administrator. The EMM Server can be configured to export the audit records to an external SYSLOG server utilizing TLS for protection of the records on the network. The EMM Server also supports the ability to query information about MDM agents and export MDM configuration information.

The EMM Agent includes the ability to the EMM Server to indicate (i.e., respond) when it has been enrolled and when it applies policies successfully. The EMM Server can be configured to alert an administrator based on its configuration. For example, it can be configured to alert he administrator when a policy update fails or an MDM Agent has been enrolled.

4.2 Cryptographic support

The EMM Server and EMM Agent both include and have access to cryptographic modules with FIPS 140-2 certified algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, initialization vector generation, secure key storage, and key and protected data destruction.

The primitive cryptographic functions are used to implement security communication protocols: TLS and HTTPS used for communication between the Server and Agent and between the Server and remote administrators.

4.3 Identification and authentication

The EMM Server authenticates mobile device users (MD users) and administrators prior to allowing those operators to perform any functions. This includes MD users enrolling their device with the EMM Server using the EMM Agent as well as an administrator logging on to manage the EMM Server configuration, MDM policies for mobile devices, etc.

In addition, both the EMM Server and Agent utilize X.509 certificates, including certificate validation checking, in conjunction with TLS to secure communications between the EMM Server and EMM Agents as well as between the EMM Server and administrators using a web-based user interface for remote administrative access.

4.4 Security management

The EMM Server is designed to two distinct user roles: administrator and Mobile Device user (MD user). The former interacts directly with the EMM Server through HTTPS (using a browser) while the latter is the user of a mobile device with the EMM Agent installed.

The EMM Server provides all the functions necessary to manage its own security functions as well as to manage mobile device policies that are sent to EMM Agents. In addition, the EMM Server ensures that security management functions are limited to authorized administrators while allowing MD users to perform only necessary functions such as enrolling with the EMM Server.

The EMM Agents provide the functions necessary to securely communicate with and enroll with the EMM Server, apply policies received from the EMM Server, and report the results of applying policies.

4.5 Protection of the TSF

The EMM Server and Agent work together to ensure that all security related communication between those components is protected from disclosure and modification.

Both the EMM Server and Agent include self-testing capabilities to ensure that they are functioning properly as well as to cryptographically verify that their executable images have not been corrupted.

The EMM Server also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.6 TOE access

The MDM Server has the capability to display an advisory banner when users attempt to login in order to manage the TOE.

4.7 Trusted path/channels

The EMM Server uses TLS/HTTPS to secure communication channels between itself and remote administrators accessing the Server via a web-based user interface. It also uses TLS to secure communication channels between itself and mobile device users (MD users). In this latter case, the protected communication channel is established between the EMM Server and EMM Agent.

5 Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for Mobile Device Management, Version 1.1, 7 March 2014 (MDMPP). That information has not been reproduced here and the MDMPP should be consulted if there is interest in that material.

The vendor has stated that the TOE will operate correctly with multiple Push Servers. That capability was outside of the scope of this evaluation. The TOE was only tested with a single Push Server, because none of the functionality specified in the functional requirements has a direct dependence on whether there are multiple Push Servers.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Mobile Device Fundamentals Protection Profile and performed by the evaluation team).
2. This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
3. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

6 Documentation

The following documentation was used as evidence for the evaluation of the Samsung SDS Co., LTD’s EMM Suite

- Samsung SDS CellWe Enterprise Mobility Management Administrator’s Guide, v1.1.0, March 2015

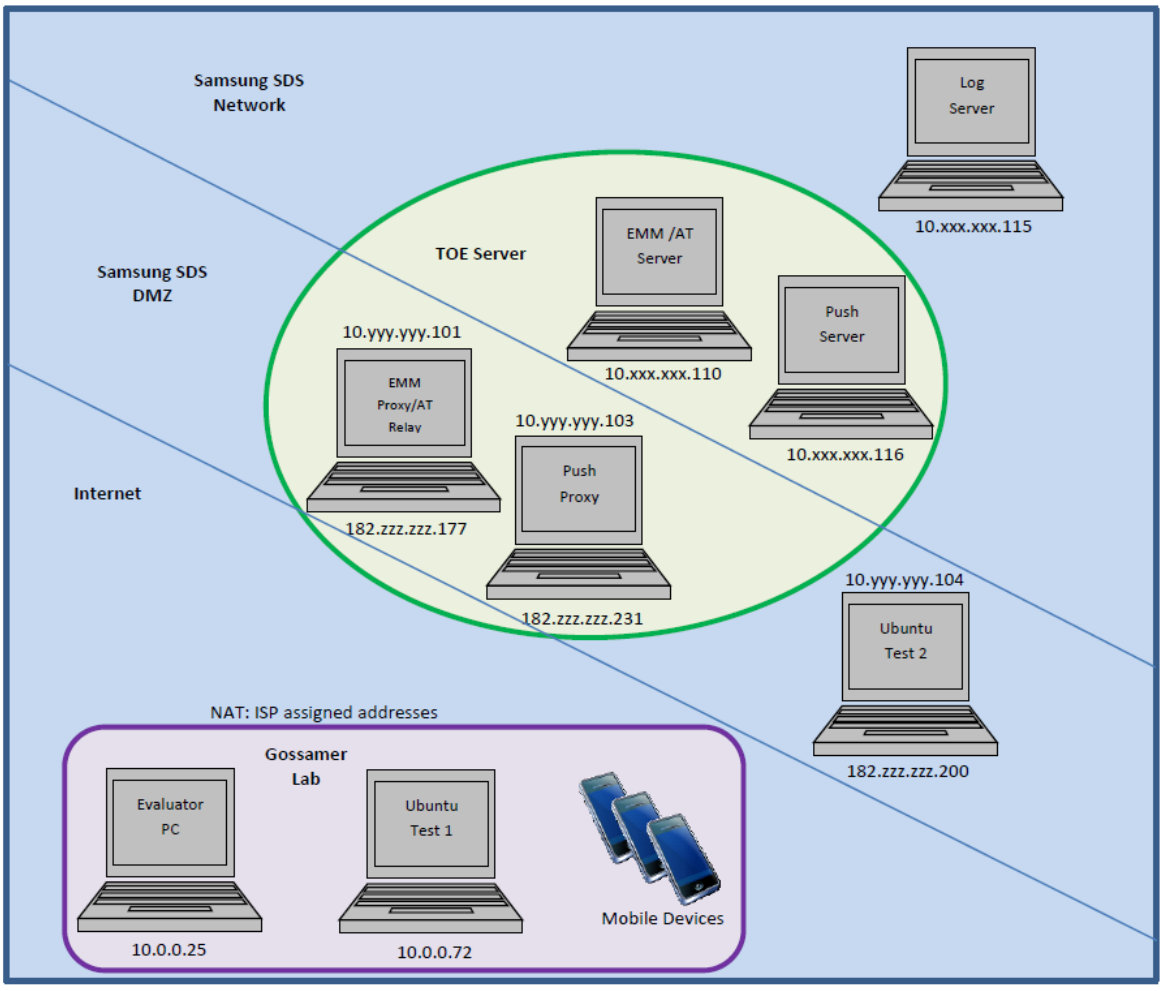
- Samsung SDS CellWe Enterprise Mobility Management User's Guide, Version 1.1.0, March 2015.
- Samsung SDS CellWe Enterprise Mobility Management Installation Guide, Version 1.1.0, March 2015

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary document: Detailed Test Report (MDMPP11) for Samsung SDS Co. Ltd CellWe EMM Suite, Version 0.5, May 8, 2015. A nonproprietary version of the tests performed and the evidence generated is summarized in the document: Assurance Activity Report (MDMPP11) for Samsung SDS Co., LTD. CellWe EMM Suite, Version 0.6, May 8, 2015.

The following diagram depicts the test environments used by the evaluators.



No evidence of developer testing is required in the assurance activities for this product.

7.1 Evaluation Team Independent Testing

The evaluation team verified the product according the Samsung SDS CellWe Enterprise Mobility Management Installation Guide, Version 1.1.0, March 2015 document and ran the tests specified in the MDMPP. The evaluation team conducted almost all testing independently of the vendor, with exception of two specific test cases, the nature of which required developer assistance. These test cases have been documented in the Assurance Activity Report (AAR), and described in detail in a corresponding Detailed Test Report (DTR) provided for the validation team's review. Some testing of the TOE was performed remotely in a vendor-provided environment. The results of those tests were confirmed and validated during independently-run testing in the evaluation team's local facility, thereby providing a high level of assurance in the accuracy of the testing results.

8 Evaluated Configuration

The evaluated configuration consists of collection of server components (MDM server) and mobile device applications (MDM agent). The MDM server was evaluated on Java 1.7 and Tomcat 7.0 running on Windows Server 2012 R2, along with SQL Server 2012 and EJBCA v 4.0.16 certificate authority. The MDM Agent was evaluated on 32-bit versions of the Android operating system, and covers evaluated Samsung devices (including the Galaxy S4, Note 3, S5, Note 4, and Galaxy Note Edge).

To use the product in the evaluated configuration, the product must be configured as specified in Samsung SDS CellWe Enterprise Mobility Management Installation Guide, Version 1.1.0, March 2015.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL1 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Samsung SDS CellWe EMM Suite version 1.1 to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement

of security requirements claimed to be met by the Samsung SDS Co., LTD EMM Suite that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the MDMPP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the MDMPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the product. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFRs within the Security Target was evaluated.

1. While the CellWe EMM suite is designed to support a wide variety of operational environments it is important to understand that testing was performed using only a limited set of the possible deployments. As explained in section 1.2 of the Assurance Activity Report, testing was performed using proxy servers in a multi-host configuration and without using any proxies in a single host configuration. While the TOE could be deployed using different combinations of hosts and proxies, including the possibility of multiple Push servers, those alternate deployment scenarios have not been tested. Furthermore, while a range of supported operating system and SQL server versions are supported and while the Assurance Activity Report explains there are no security dependencies in each case, users should be aware that testing has been conducted using only the latest versions in each case.
2. As explained in section 3.4.1 of the Assurance Activity Report, the evaluators performed much of their testing in an environment hosted by the product developer. While the evaluators had significant access to that environment, their level of

control was less than absolute given the nature of the configuration. Consequently, in order to add assurance and independence in the overall test results, the evaluators substantially repeated the test cases using an alternate TOE configuration installed and controlled within the evaluator's laboratory.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Samsung SDS Co., LTD EMM Suite (MDMPP11) Security Target, Version 0.6, May 8, 2015*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Mobile Device Management, Version 1.1, 7 March 2014.

[5] Assurance Activity Report (MDMPP11) for Samsung SDS Co., LTD. CellWe EMM Suite, Version 0.6, May 8, 2015

[6] Samsung SDS Co., LTD EMM Suite (MDMPP11) Security Target, Version 0.6, May 8, 2015

[7] Detailed Test Report (MDMPP11) for Samsung SDS Co. Ltd CellWe EMM Suite, Version 0.5, May 8, 2015