National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Samsung SDS Co., LTD

Samsung SDS Tower, 125, Olympic-ro 35-gil, Songpa-gu

Seoul, Korea 138-240

Samsung SDS EMM

Report Number: CCEVS-VR-VID10751-2016
Dated: December 29, 2016
Version: 1.0

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

Sheldon Durrant
MITRE Corporation,
Bedford, MA

Jerome Myers
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

James Arnold
Cornelius Haley
Raymond Smoley
Catherine Sykes
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 EMM solution 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 December 2016. 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 Samsung SDS EMM.

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 EMM (MDMPP20/MDMAEP20) Security Target, version 0.4, December 22, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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) for Evaluation Assurance Level (EAL) 1 through 4 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 EMM 1.5.1 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Mobile Device Management, Version 2.0, 31 December 2014 (MDMPP20) and Extended Package for Mobile Device Management Agents, Version 2.0, 31 December 2014 (MDMAEP20)
ST	Samsung SDS Co., LTD EMM (MDMPP20/MDMAEP20) Security Target, Version 0.4, 2016/12/22
Evaluation Technical Report	Evaluation Technical Report for Samsung SDS EMM 1.5.1, version 0.2, December 29, 2016
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	Sheldon Durrant, MITRE Corporation
	Jerome Myers, Aerospace Corporation

3 Architectural Information

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

Samsung SDS offers the EMM Server as a software installation for Java 1.8 and Tomcat 7.0 running on the Microsoft Windows Server 2012 or Windows Server 2012 R2 operating system. 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 6.2 cryptographic module as part of its software, and the EMM Server's Microsoft Windows platform includes SQL server 2008-2014 and a Microsoft CA certificate authority.

Samsung SDS provides the EMM Agent software for evaluated Samsung mobile devices and for evaluated Apple mobile devices. 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.

The Target of Evaluation (TOE) is Samsung SDS Co., LTD EMM.

The SDS EMM 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.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

1) The EMM Server (version 1.5.1) installed upon the Microsoft Windows 2012 R2 operating system with Oracle JRE 1.8, Microsoft SQL Server 2014, and Microsoft's Certificate Authority (CA).
2) The EMM Client version 1.5.1 APKs (EMM Agent, PushAgent, and EMM Agent Resource) installed upon a Samsung Galaxy Note 4, S6, and S7 running Android 6.0.1.
3) The EMM Client version 1.5.1 application installed upon an iPhone 5s.

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 (a single Push Server configuration was used during testing).
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 administrators to create and enforce two different types of profiles:

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

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 Agent consists of a single component on evaluated iOS platforms:

1. The EMM application – this iOS application provides a user interface to allow the user to enroll their phone with their organization's SDS EMM Server. The application relies upon the evaluated, embedded Apple agent for all agent functionality.

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 SDS EMM 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 a MS CA.

4 Security Policy

This section summaries 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 either in CSV (comma separated values) from the console through its HTTPS interface, or in file-based format accessible through RDP to the EMM Server's platform. In both cases, the EMM Server protects the exported audit records using TLS (as part of HTTPS and RDP). 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 indicate (i.e., respond) to the EMM Server 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 the 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 Cryptographic Algorithm Validation Program (CAVP) certified algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, encryption/decryption, and 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 with 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 function 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 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

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Mobile Device Management, Version 2.0, 31 December 2014 (MDMPP20)
- Extended Package for Mobile Device Management Agents, Version 2.0, 31 December 2014 (MDMAEP20)

That information has not been reproduced here and the MDMPP20/MDMAEP20 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the MDMPP20/MDMAEP20 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

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:

- 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.
- 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.

7 Documentation

The following documents were available with the TOE for evaluation:

- Samsung SDS EMM Administrator’s Guide, Version 1.5.1, December 2016

- Samsung SDS EMM Installation Guide, Version 1.5.1, December 2016
- Samsung Push Installation Guide, Version 1.5.1, December 2016
- Samsung AppTunnel Installation Guide, Version 1.5.1, December 2016

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (MDMPP20/MDMAEP20) for EMM, Version 0.2, December 19, 2016 (DTR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the MDMPP20/MDMAEP20 including the tests associated with optional requirements.

9 Evaluated Configuration

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

To use the product in the evaluated configuration, the product must be configured as specified in Samsung SDS EMM Installation Guide, Version 1.5.1, December 2016.

10 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 Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

10.1 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 EMM 1.5.1 products 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.

10.2 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 MDMPP20/MDMAEP20 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.

10.3 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.

10.4 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.

10.5 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 MDMPP20/MDMAEP20 and recorded the results in a Test Report, summarized in the AAR.

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.

10.6 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.

10.7 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.

11 Validator Comments/Recommendations

As described earlier in this document, the Samsung SDS EMM was evaluated against two NIAP Protection Profiles, the MDMPP20 for the MDM server component, and the MDMAEP20 for the MDM Agent component for Android devices. In addition, the MDM server component was tested against the MDM agent capability provided as part of Apple's iOS operating system and evaluated by NIAP. Given the differences between the functionality provided by the Samsung agent versus the Apple agent, the ST for this evaluation explicitly highlights which set of functionality and corresponding SFRs are satisfied by the Samsung agent versus the embedded Apple agent.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Samsung SDS EMM (MDMPP20/MDMAEP20) Security Target, Version 0.4, December 22, 2016.*

14 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.

15 **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 2.0, 31 December 2014 (MDMPP20) and Extended Package for Mobile Device Management Agents, Version 2.0, 31 December 2014 (MDMAEP20)

[5] Samsung SDS EMM (MDMPP20/MDMAEP20) Security Target, Version 0.4, December 22, 2016 (ST)

[6] Assurance Activity Report (MDMPP20/MDMAEP20) for EMM, Version 0.2, December 19, 2016 (AAR)

[7] Detailed Test Report (MDMPP20/MDMAEP20) for EMM, Version 0.2, December 19, 2016 (DTR)

[8] Evaluation Technical Report for Samsung SDS EMM 1.5.1, ETR Version 0.2, December 29, 2016 (ETR)