National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Samsung SDS EMM and EMM Agent for Android 2.2.5

Report Number: CCEVS-VR-VID11362-2023
Dated: June 16 , 2023
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, Ph.D.
Jerome Myers, Ph.D.
J. David Thompson
The Aerospace Corporation

Anne Gugel
John Hopkins University APL

Common Criteria Testing Laboratory

Tammy Compton
Douglas Kalmus
Rizheng Sun
Gossamer Security Solutions, Inc.
Columbia, 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 and EMM Agent for Android 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 Columbia, MD, United States of America, and was completed in June 2023. 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 the PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, January 27, 2020 (CFG_MDM-MDM_AGENT_V1.0) which includes the base PP: Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40) with the PP-Module for MDM Agents, Version 1.0, 25 April 2019 (MDMA10) and the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)].

The Target of Evaluation (TOE) is the Samsung SDS EMM and EMM Agent for Android 2.2.5.

The 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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 technical information included in this report was obtained from the Samsung SDS EMM and EMM Agent for Android 2.2.5 Security Target, version 0.92, May 26, 2023 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) 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 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 and EMM Agent for Android 2.2.5 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, January 27, 2020 (CFG_MDM-MDM_AGENT_V1.0) which includes the base PP: Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40) with the PP_Module for MDM Agents, Version 1.0, 25 April 2019 (MDMA10) and the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)]
ST	Samsung SDS EMM and EMM Agent for Android 2.2.5 Security Target, version 0.92, May 26, 2023
Evaluation Technical Report	Evaluation Technical Report for Samsung SDS EMM and EMM Agent for Android 2.2.5, version 0.1, May 31, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Samsung SDS Co., LTD

Item	Identifier
Developer	Samsung SDS Co., LTD
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Patrick Mallett, Jerome Myers, David Thompson, Anne Gugel

3 Architectural Information

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

The TOE is Samsung SDS EMM and EMM Agent for Android version 2.2.5[1].

The SDS EMM provides centralized management of mobile devices and the EMM Agent for Android (installed on each device) enforces the policies of the Server on each device. Samsung SDS offers the EMM as a software installation for Java 1.8 running on the Microsoft Windows Server 2016 or Windows Server 2019 operating system. Once installed, the EMM allows administrators to configure policies for devices and also serves as a Mobile Application Store (MAS) server to serve configured applications to enrolled devices. Administrators connect securely to the EMM using a web browser (whether local to the Server itself or remote) and through the EMM's web interface can enroll, audit, lock, unlock, manage, and set policies for enrolled mobile devices. The EMM includes the RSA Crypto-J 6.3 cryptographic module as part of its software, and the EMM's Microsoft Windows platform includes SQL server 2008-2016, 2019 and a Microsoft Certificate Authority.

Note that one can install multiple EMM systems in order to allow the overall solution to scale the supported number of mobile devices as a High Availability (HA) option. In this case, the multiple EMM systems can operate concurrently and with the same policies and other information by sharing the same SQL database.

Samsung SDS provides the EMM Agent for Android software for evaluated Samsung mobile devices. The EMM Agent software, once installed and enrolled with the EMM, will apply and enforce administrator configured policies communicated through the EMM to the EMM Agent's running on the mobile devices. The scope of supported EMM Agent for Android devices for the evaluation will be limited by the set of devices evaluated on the NIAP PCL (refer to the following evaluations).

During evaluation testing EMM Server and EMM Agent were tested in the following configuration:

- Android 13 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11342,
- Android 12 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11307,
- Android 12 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11228, and

[1] Note that while the EMM Server and Android Agent are version 2,2.5, the supporting Push Agent for Android is version 2.5.1.

- Android 11 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11211.

While Samsung SDS does not provide an iOS agent, the EMM is designed to work with the iOS agents developed and evaluated by Apple. Since the iOS agents are evaluated as part of the Apple iOS evaluations, the EMM was tested only to ensure it can manage those devices, but the agent's behavior on those devices was not otherwise tested. The support is limited by the set of devices evaluated on the NIAP PCL (ref.

- iOS 15 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11237, and
- iOS 16 - https://www.niap-ccevs.org/Product/PINE.cfm (in progress - VID 11349) .

3.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The EMM actually consists of the following different servers (these components are referred to collectively as EMM throughout subsequent sections of this document):

1. EMM Server – This is the main server running to which remote administrators connect. The EMM Server bears responsibility for all logic needed to manage mobile devices and to serve configured applications as a MAS server. When multiple EMM Servers are configured in a single operational environment, they are not directly associated or communicating with each other, but rather can simply share the same SQL database. The EMM Server is installed as a single component, but includes an integrated Tomcat server to implement the administrator Web User Interface and also an integrated Push server implementation (PUSH_SA) used to communicate with the other EMM server components (Push and AppTunnel).
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. Each Push Server is installed as a single component, but includes multiple internal modules (DCM/PS/SCM/ECM/ICM) to implement its full range of communication channels among EMM components and agents.
    a. Push Proxy – This is an alternate optional deployment of the Push Server that serves to relay or proxy messages between the mobile devices and Push Server. This deployment would normally be used to accommodate network architectures with DMZs. Each Push Proxy is installed as a single alternate deployment of the Push Server and also includes multiple internal modules (DPP/PPP/EPP) to implement its full range of communication channels among EMM components and agents in its proxy role.
3. AppTunnel (AT) Server – this server accepts connections from the EMM Agent (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. Each

AT Server is installed as a single component and includes only a single module to implement its role of managing secure channels for apps.

a. AT Relay – This is an alternate optional deployment of the AppTunnel Server that serves to relay or proxy messages between the mobile devices and AT Server. This deployment would normally be used to accommodate network architectures with DMZs. Each AT Relay is installed as a single alternate deployment of the AT Server and also includes only a single module to implement its role of relaying secure channels for apps.

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

The minimum deployment for an EMM is an EMM Server, a Push Server, and an AT Server. While each EMM Server is paired with an AT Server, multiple Push Servers can optionally be configured to operate with a single EMM Server. Also optionally, a Push Proxy can be configured for each Push Server and an AT Relay can be configured for the AT Server. The majority of EMM security functions are implemented in the EMM Server while the other server components are primarily responsible for secure communications between the EMM Server and the enrolled device agents (see **Error! Reference source not found.**).

The EMM Agent for Android consists of two different components on evaluated Android platforms (these components are referred to collectively as EMM Agent throughout subsequent sections of this document):

1. The "EMM Agent" – 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. The EMM Agent presents the UI to allow users to start the enrollment process and, once enrolled, to log in and log out. This component also 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 enforces the policies of the Server.
2. 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 TOE includes a single component on evaluated iOS platforms:

1. The EMM Client – this iOS application provides a user interface to allow the user to enroll their phone with their organization's SDS EMM. The application relies upon the evaluated, embedded Apple agent for all agent functionality. As such, this component doesn't provide any security functions.

3.3 Physical Boundaries

The physical boundaries of the SDS EMM and EMM Agent for Android are the physical perimeter of the servers hosting the EMM server components and the physical perimeter of the mobile devices being managed by the EMM (put another way, the mobile devices running the EMM Agent).

The EMM 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 can generate and store audit records for security-relevant events as they occur. These events are stored and protected by the EMM and can be reviewed by an authorized administrator. The EMM can export the majority of audit events directly through the HTTPS protected GUI in a CSV format. Some low-level events are maintained in text files on the TOE platform and can be exported via RDP using the TOE platform. In both cases, the EMM protects the exported audit records using TLS (as part of HTTPS and RDP). The EMM 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 when it has been enrolled and when it applies policies successfully. The EMM 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 and EMM Agent both include or 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 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 using the EMM Agent as well as an administrator logging on to manage the EMM configuration, MDM policies for mobile devices, etc.

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

4.4 Security management

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

The EMM 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 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.

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

4.5 Protection of the TSF

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

Both the EMM 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 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 uses TLS/HTTPS to secure communication channels between its distributed components 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 and EMM Agent.

5 Assumptions & Clarification of Scope

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

- Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40)
- PP_Module for MDM Agents, Version 1.0, 25 April 2019 (MDMA10)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)]

That information has not been reproduced here and the MDMPP40/MDMA10/PKGTLS11 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 MDMPP40/MDMA10/PKGTLS11 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.

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:

- 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 Management Protection Profile with the MDM Agents PP-Module and the TLS Package and performed by the evaluation team).
- 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.
- Apart from the Admin Guide, additional customer documentation for the specific Mobile Device Management models was not included in the scope of the evaluation

and therefore should not to be relied upon when configuring or operating the device as evaluated.

- 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.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the MDMPP40/MDMA10/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Samsung EMM Administrator's Guide, Version Solution version 2.2.5, January 2023
- Samsung SDS EMM Installation Guide, Version Solution version 2.2.5, January 2023
- Samsung SDS EMM Configuration Guide for IPsec settings in Microsoft Windows Server 2016/2019 for Common Criteria Evaluation, Solution version 2.2.5, January 27, 2023

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured 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 Detailed Test Report for Samsung SDS EMM and EMM Agent for Android, Version 0.1, May 31, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the MDMPP40/MDMA10/PKGTLS11 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration consists of the hardware and software listed below when configured in accordance with the documentation specified in section 6. The evaluated configuration consists of the following models:

1) The EMM Server components (version 2.2.5) installed upon the Microsoft Windows Server 2016 or 2019 operating system with Java 1.8, Microsoft SQL Server 2008-2016 or 2019, and Microsoft's Certificate Authority (CA).
2) The EMM Client version 2.2.5 APKs (EMM Agent, PushAgent[2], and EMM Agent Resource) installed upon an evaluated Samsung device running Android 11, 12, or 13. (see Security Target for a mapping to Samsung mobile device evaluations)
3) The EMM Client version 2.2.5 application installed upon an evaluated iPhone running iOS 15 or 16. (see Security Target for a mapping to Apple mobile device evaluations)

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 assurance activities and 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 5 and CEM version 3.1 rev 5. The evaluation determined the EMM and EMM Agent for Android TOE to be Part 2 extended, and to meet the SARs contained in the MDMPP40/MDMA10/PKGTLS11.

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 EMM and EMM Agent for Android 2.2.5 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

[2] Note that while the EMM Agent and EMM Agent Resource are version 2,2.5, the supporting Push Agent for Android is version 2.5.1

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 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 MDMPP40/MDMA10/PKGTLS11 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 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 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 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the MDMPP40/MDMA10/PKGTLS11 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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories), Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 5/30/2023 with the following search terms: "Crypto-J", "CryptoJ", "Crypto J", "SDS", "Enterprise Mobility Management", "EMM".

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 validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guides listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Samsung SDS EMM and EMM Agent for Android 2.2.5 Security Target, Version 0.92, May 26, 2023*.

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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40

[5] PP_Module for MDM Agents, Version 1.0, 25 April 2019 (MDMA10)

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)].

[7] Samsung SDS EMM and EMM Agent for Android 2.2.5 Security Target, Version 0.92, May 26, 2023 (ST).

[8] Assurance Activity Report for Samsung SDS EMM and EMM Agent for Android 2.2.5, Version 0.1, May 31, 2023 (AAR).

[9] Detailed Test Report for Samsung SDS EMM and EMM Agent for Android 2.2.5, Version 0.1, May 31, 2023 (DTR).

[10] Evaluation Technical Report for Samsung SDS EMM and EMM Agent for Android, Version 0.1, May 31, 2023 (ETR)