National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Mobile Device Management

Version 4.0

25 April 2019

Report Number: CCEVS-VR-PP-0061
Dated: 14 February 2020
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

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Mobile Device Management, Version 4.0 (PP_MDM_V4.0). It presents a summary of the PP_MDM_V4.0 and the evaluation results.

Gossamer Security Solutions, located in Catonsville, Maryland, performed the evaluation of PP_MDM_V4.0 concurrent with the first product evaluation against the PP's requirements. The evaluated product was Samsung SDS Co. Ltd. EMM and EMM Agent for Android.

This evaluation addressed the base requirements of PP_MDM_V4.0 and several of the additional requirements contained in Appendices A, B, and C.

The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined that PP_MDM_V4.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from the PP_MDM_V4.0; completion of the ASE work units satisfied the APE work units for PP_MDM_V4.0, but only for those parts of the ST that were relevant to this PP. The ST also claims conformance to the PP-Module for Mobile Device Management Agents and TLS Package, but these materials are separate from PP_MDM_V4.0 and are therefore outside the scope of this VR.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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 CCTLs. CCTLs evaluate products against PPs that contain Evaluation Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of PP_MDM_V4.0 was performed concurrent with the first product evaluation against the PP's requirements. In this case, the Target of Evaluation (TOE) was Samsung SDS Co. Ltd. EMM and EMM Agent for Android, evaluated by Gossamer Security Solutions in Catonsville, Maryland, United States of America.

These evaluations addressed the base requirements of PP_MDM_V4.0, and several of the additional requirements contained in Appendices A, B, and C.

PP_MDM_V4.0 contains a set of base requirements that all conformant STs must include, and additionally contains optional, selection-based, and objective requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

A specific ST may not include all non-base requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ work units performed against PP_MDM_V4.0. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include references to this as additional evidence that the corresponding portions of PP_MDM_V4.0 were evaluated.

The following identifies the PP subject of the evaluation or validation, as well as the supporting information from the evaluation performed against this PP.

Protection Profile	Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019
ST (Base)	Samsung SDS Co. Ltd. EMM and EMM Agent for Android Security Target, Version 0.9, 27 January 2020
Assurance Activity Report (Base)	Assurance Activity Report (MDMPP40/MDMA10/PKGTLS11) for Samsung SDS Co. Ltd. EMM and EMM Agent for Android, Version 0.3, 27 January 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Gossamer Security Solutions Catonsville, Maryland 21228

3 PP_MDM_V4.0 Description

The PP_MDM_V4.0 specifies information security requirements for mobile device management, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE, which is referred to as an “MDM” or “MDM Server.”

The MDM Server is software (an application, service, etc.) on a general-purpose platform, a network device, or cloud architecture executing in a trusted network environment. The MDM Server provides administration of the mobile device policies and reporting on mobile device behavior. The MDM Server is responsible for managing device enrollment, configuring and sending policies to the MDM Agents, collecting reports on device status, and sending commands to the Agents. The MDM Server may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfill the requirements of the PP.

The MDM may also include a Mobile Application Store (MAS), which hosts applications for the enterprise, authenticates Agents, and securely transmits applications to enrolled mobile devices. The MAS functionality can be included as part of the MDM Server Software or can be logically distinct. If the MAS functionality is on a physically separate server, then the TOE is distributed with the MDM Server and MAS Server being separate components.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.CONNECTIVITY	The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
A.MDM_SERVER_PLATFORM	The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities. The MDM Server relies on this platform to provide a range of security-related services including reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.
A.PROPER_USER	One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
A.PROPER_ADMIN	Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.MALICIOUS_APPS	Malicious or flawed application threats exist because apps loaded onto a mobile device may include malicious or exploitable code. An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE, resulting in the compromise of TOE or TOE data.
T.NETWORK_ATTACK	An attacker may masquerade as an MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.

Threat Name	Threat Definition
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the MDM Server and other endpoints.
T.PHYSICAL_ACCESS	The mobile device may be lost or stolen, and an unauthorized individual may attempt to access user data. Although these attacks are primarily directed against the mobile device platform, the TOE configures features, which address these threats.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Threats

Threat Name	Threat Definition
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.
P.ADMIN	The configuration of the mobile device security functions must adhere to the Enterprise security policy.
P.DEVICE_ENROLL	A mobile device must be enrolled for a specific user by the administrator of the MDM prior to being used in the Enterprise network by the user.
P.NOTIFY	The mobile user must immediately notify the administrator if a mobile device is lost or stolen so that the administrator may apply remediation actions via the MDM system.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
O.ACCOUNTABILITY	The TOE must provide logging facilities which record management actions undertaken by its administrators.
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the mobile OS and the MDM Server. This will include the initial enrollment of the device into management through its entire lifecycle, including policy updates and its possible unenrollment from management services.
O.DATA_PROTECTION_TRANSIT	Data exchanged between the MDM Server and the MDM Agent must be protected from being monitored, accessed, or altered.
O.INTEGRITY	The TOE will provide the capability to perform self tests to ensure the integrity of critical functionality, software, firmware, and data has been maintained. The TOE will also provide a means to verify the integrity of downloaded updates.
O.MANAGEMENT	The TOE provides access controls around its management functionality.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex

TOE Security Objective	TOE Security Objective Definition
	operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
OE.COMPONENTS_RUNNING	For distributed TOEs the administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.PROPER_USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.
OE.IT_ENTERPRISE	The enterprise IT infrastructure provides security for a network that is available to the TOE and mobile devices that prevents unauthorized access.
OE.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.

5 Functional Requirements

As indicated above, requirements in the PP_MDM_V4.0 are comprised of the "base" requirements and additional requirements that are optional, selection-based, or objective. The following table contains the "base" requirements that were validated as part of the Gossamer Security Solutions evaluation activities referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ALT_EXT.1: Server Alerts	Samsung SDS EMM and EMM Agent for Android
	FAU_GEN.1(1): Audit Data Generation	Samsung SDS EMM and EMM Agent for Android
	FAU_NET_EXT.1: Network Reachability Review	Samsung SDS EMM and EMM Agent for Android
	FAU_STG_EXT.1: External Trail Storage	Samsung SDS EMM and EMM Agent for Android
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Samsung SDS EMM and EMM Agent for Android
	FCS_CKM.2: Cryptographic Key Establishment	Samsung SDS EMM and EMM Agent for Android
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Samsung SDS EMM and EMM Agent for Android
	FCS_COP.1(1): Cryptographic Operation (Confidentiality Algorithms)	Samsung SDS EMM and EMM Agent for Android
	FCS_COP.1(2): Cryptographic Operation (Hashing Algorithms)	Samsung SDS EMM and EMM Agent for Android
	FCS_COP.1(3): Cryptographic Operation (Signature Algorithms)	Samsung SDS EMM and EMM Agent for Android
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)	Samsung SDS EMM and EMM Agent for Android
	FCS_RBG_EXT.1: Extended: Random Bit Generation	Samsung SDS EMM and EMM Agent for Android
	FCS_STG_EXT.1: Cryptographic Key Storage	Samsung SDS EMM and EMM Agent for Android
FIA: Identification and Authentication	FIA_ENR_EXT.1: Enrollment of Mobile Device into Management	Samsung SDS EMM and EMM Agent for Android
	FIA_UAU.1: Timing of Authentication	Samsung SDS EMM and EMM Agent for Android
	FIA_X509_EXT.1(1): X.509 Certificate Validation	Samsung SDS EMM and EMM Agent for Android
	FIA_X509_EXT.2: X.509 Certificate Authentication	Samsung SDS EMM and EMM Agent for Android
	FIA_X509_EXT.5: X.509 Unique Certificate	Samsung SDS EMM and EMM Agent for Android
FMT: Security Management	FMT_MOF.1(1): Management of Functions Behavior	Samsung SDS EMM and EMM Agent for Android
	FMT_MOF.1(2): Management of Functions Behavior (Enrollment)	Samsung SDS EMM and EMM Agent for Android

Requirement Class	Requirement Component	Verified By
	FMT_POL_EXT.1: Trusted Policy Update	Samsung SDS EMM and EMM Agent for Android
	FMT_SMF.1(1): Specification of Management Functions (Server configuration of Agent)	Samsung SDS EMM and EMM Agent for Android
	FMT_SMF.1(2): Specification of Management Functions (Server Configuration of Server)	Samsung SDS EMM and EMM Agent for Android
	FMT_SMR.1(1): Security Management Roles	Samsung SDS EMM and EMM Agent for Android
FPT: Protection of the TSF	FPT_API_EXT.1: Use of Supported Services and APIs	Samsung SDS EMM and EMM Agent for Android
	FPT_LIB_EXT.1: Use of Third Party Libraries	Samsung SDS EMM and EMM Agent for Android
	FPT_TST_EXT.1: Functionality Testing	Samsung SDS EMM and EMM Agent for Android
	FPT_TUD:_EXT.1 Trusted Update	Samsung SDS EMM and EMM Agent for Android
FTP: Trusted Path/Channel	FTP_ITC_EXT.1: Trusted Channel	Samsung SDS EMM and EMM Agent for Android
	FTP_ITC.1(1): Inter-TSF Trusted Channel (Authorized IT Entities)	Samsung SDS EMM and EMM Agent for Android
	FTP_TRP.1(1): Trusted Path (for Remote Administration)	Samsung SDS EMM and EMM Agent for Android
	FTP_TRP.1(2): Trusted Path (for Enrollment)	Samsung SDS EMM and EMM Agent for Android

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SAR.1: Audit Review	Samsung SDS EMM and EMM Agent for Android
	FAU_SEL.1: Security Audit Event Selection	PP Evaluation
FTA: TOE Access	FTA_TAB.1: Default TOE Access Banners	Samsung SDS EMM and EMM Agent for Android

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1(2): Audit Generation (MAS Server)	Samsung SDS EMM and EMM Agent for Android

Requirement Class	Requirement Component	Verified By
	FAU_STG_EXT.2: Audit Event Storage	Samsung SDS EMM and EMM Agent for Android
FCS: Cryptographic Support	FCS_HTTPS_EXT.1: HTTPS Protocol	Samsung SDS EMM and EMM Agent for Android
	FCS_IV_EXT.1: Initialization Vector Generation	Samsung SDS EMM and EMM Agent for Android
	FCS_STG_EXT.2: Encrypted Cryptographic Key Storage	Samsung SDS EMM and EMM Agent for Android
FIA: Identification and Authentication	FIA_X509_EXT.1(2): X.509 Certificate Validation	Samsung SDS EMM and EMM Agent for Android
FMT: Security Management	FMT_MOF.1(3): Management of Functions in (MAS Server Downloads)	Samsung SDS EMM and EMM Agent for Android
	FMT_SMF.1(3): Specification of Management Functions (MAS Server)	Samsung SDS EMM and EMM Agent for Android
	FMT_SMR.1(2): Security Management Roles (MAS Server)	Samsung SDS EMM and EMM Agent for Android
FPT: Protection of the TSF	FPT_ITT.1(1): Internal TOE TSF Data Transfer	Samsung SDS EMM and EMM Agent for Android
	FPT_ITT.1(2): Internal TOE TSF Data Transfer (MDM Agent)	Samsung SDS EMM and EMM Agent for Android
FTP: Trusted Path/Channels	FTP_ITC.1(2): Inter-TSF Trusted Channel (MDM Agent)	Samsung SDS EMM and EMM Agent for Android

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_CRP_EXT.1: Support for Compliance Reporting of Mobile Device Configuration	PP Evaluation
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	PP Evaluation
FIA: Identification and Authentication	FIA_UAU_EXT.4(1): User Authentication (Re-Use Prevention)	PP Evaluation
	FIA_UAU_EXT.4(1): User Authentication (Re-Use Prevention)	PP Evaluation
	FIA_X509_EXT.3: X.509 Enrollment	PP Evaluation
	FIA_X509_EXT.4: Alternate X.509 Enrollment	PP Evaluation
FMT: Security Management	FMT_SAE_EXT.1: Security Attribute Expiration	PP Evaluation
FTP: Trusted Path/Channels	FTP_TRP.1(3): Trusted Path (for Joining)	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the PP_MDM_V4.0.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ADV: Development	ADV_FSP.1 Basic Functional Specification	Samsung SDS EMM and EMM Agent for Android
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Samsung SDS EMM and EMM Agent for Android
	AGD_PRE.1: Preparative Procedures	Samsung SDS EMM and EMM Agent for Android
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Samsung SDS EMM and EMM Agent for Android
	ALC_CMS.1: TOE CM Coverage	Samsung SDS EMM and EMM Agent for Android
ASE: Security Target	ASE_CCL.1: Conformance Claims	Samsung SDS EMM and EMM Agent for Android
	ASE_ECD.1: Extended Components Definition	Samsung SDS EMM and EMM Agent for Android
	ASE_INT.1: ST Introduction	Samsung SDS EMM and EMM Agent for Android
	ASE_OBJ.1: Security Objectives	Samsung SDS EMM and EMM Agent for Android
	ASE_REQ.1: Security Requirements	Samsung SDS EMM and EMM Agent for Android
	ASE_TSS.1: TOE Summary Specifications	Samsung SDS EMM and EMM Agent for Android
ATE: Tests	ATE_IND.1: Independent Testing – Sample	Samsung SDS EMM and EMM Agent for Android
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Samsung SDS EMM and EMM Agent for Android

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 11: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	PP Evaluation
APE_ECD.1	Pass	PP Evaluation
APE_INT.1	Pass	PP Evaluation
APE_OBJ.1	Pass	PP Evaluation
APE_REQ.1	Pass	PP Evaluation
APE_SPD.1	Pass	PP Evaluation

8 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 as interpreted by the supplemental guidance in the PP_MDM_V4.0 Evaluation Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019.

[7] Samsung SDS Co. Ltd. EMM and EMM Agent for Android Security Target, Version 0.9, 27 January 2020

[8] Assurance Activity Report (MDMPP40/MDMA10/PKGTLS11) for Samsung SDS Co. Ltd. EMM and EMM Agent for Android, Version 0.3, 27 January 2020