National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Mobile Device Management (MDM) and MDM Agents

Version 1.0

25 April 2020

Report Number: CCEVS-VR-PP-0062
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 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 PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0 (CFG_MDM-MDM_AGENT_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Mobile Device Management (PP_MDM_V4.0) Base-PP and the PP-Module for MDM Agent, Version 1.0 (MOD_MDM_AGENT_V1.0). It presents a summary of the CFG_MDM-MDM_AGENT_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Catonsville, Maryland, performed the evaluation of the CFG_MDM-MDM_AGENT_V1.0 and MOD_MDM_AGENT_V1.0 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Samsung SDS Co. Ltd. EMM and EMM Agent for Android.

This evaluation addressed the base security functional requirements of MOD_MDM_AGENT_V1.0 as part of CFG_MDM-MDM_AGENT_V1.0. The Module defines additional requirements but the Samsung evaluation did not claim any of these.

The Validation Report (VR) author independently performed an additional review of the PP-Configuration and Module as part of the completion of this VR, to confirm they meet the claimed ACE requirements.

The evaluation determined the CFG_MDM-MDM_AGENT_V1.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration and Module identified in this VR 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 both PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0; completion of the ASE work units satisfied the ACE work units for this Module, but only for the materials defined in this Module, and only when the Module is in the defined PP-Configuration. The ST also claims conformance to the TLS Package, but these materials are separate from CFG_MDM-MDM_AGENT_V1.0 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 Protection Profiles (PPs) and Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or Module. Products may only be evaluated against Modules when a PP-Configuration is defined to include the Module with at least one corresponding Base-PP.

In order to promote thoroughness and efficiency, the evaluation of the CFG_MDM-MDM_AGENT_V1.0 and MOD_MDM_AGENT_V1.0 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Samsung SDS Co. Ltd. EMM and EMM Agent for Android, performed by Gossamer Security Solutions in Catonsville, Maryland, United States.

This evaluation addressed the base security functional requirements of MOD_MDM_AGENT_V1.0 as part of CFG_MDM-MDM_AGENT_V1.0. The Module defines additional requirements but the Samsung evaluation did not claim any of these.

MOD_MDM_AGENT_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains objective requirements. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the Module. 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 reference to this as additional evidence that the corresponding portions of the CFG_MDM-MDM_AGENT_V1.0 were evaluated.

The following identifies the Module in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this Module.

PP-Configuration	PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, 27 January 2020
Module(s) in PP-Configuration	PP-Module for MDM Agents, Version 1.0, 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 CFG_MDM-MDM_AGENT_V1.0 Description

CFG_MDM-MDM_AGENT_V1.0 is a PP-Configuration that combines the following:

- Protection Profile for Mobile Device Management, Version 4.0 (PP_MDM_V4.0)
- Protection Profile Module for MDM Agents, Version 1.0 (MOD_MDM_AGENT_V1.0)

The PP-Configuration defines a baseline set of security functional requirements (SFRs) for mobile device management applications (defined in PP_MDM_V4.0) that are bundled with agent applications to enforce configured policies on mobile devices (defined in MOD_MDM_AGENT_V1.0).

An MDM Agent establishes a secure connection back to the MDM Server, from which it receives policies to enforce on the mobile device. Optionally, the MDM Agent interacts with the Mobile Application Store (MAS) Server to download and install enterprise-hosted applications.

An MDM Agent may also be bundled as part of a mobile device operating system. In this case, it would be evaluated with the Protection Profile for Mobile Device Fundamentals as its Base-PP, which is outside the scope of CFG_MDM-MDM_AGENT_V1.0.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_MDM-MDM_AGENT_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_MDM_V4.0	
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.
From MOD_MDM_AGENT_V1.0	
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.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon mobile platform and hardware evaluated against the MDF PP and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
A.PROPER_ADMIN	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_USER	Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_MDM-MDM_AGENT_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From PP_MDM_V4.0	
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.
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.
From MOD_MDM_AGENT_V1.0	
T.BACKUP	An attacker may try to target backups of data or credentials and exfiltrate data. Since the backup is stored on either a personal computer or end user's backup repository, it's not likely the enterprise would detect compromise.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_MDM-MDM_AGENT_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_MDM_V4.0	
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.
From MOD_MDM_AGENT_V1.0	
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.

OSP Name	OSP Definition
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

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_MDM-MDM_AGENT_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_MDM_V4.0	
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 operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
From MOD_MDM_AGENT_V1.0	
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.STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of a mobile device (T.PHYSICAL), conformant TOEs will use

TOE Security Objective	TOE Security Objective Definition
	platform provide key storage. The TOE is expected to protect its persistent secrets and private keys.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_MDM-MDM_AGENT_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_MDM_V4.0	
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.
From MOD_MDM_AGENT_V1.0	
OE.DATA_PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.DATA_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-MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon the trustworthy mobile platform and hardware to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.

5 Functional Requirements

As indicated above, CFG_MDM-MDM_AGENT_V1.0 includes both PP_MDM_V4.0 and MOD_MDM_AGENT_V1.0. The functional requirements from PP_MDM_V4.0 were evaluated separately so this section applies only to requirements of MOD_MDM_AGENT_V1.0.

As indicated above, requirements in the MOD_MDM_AGENT_V1.0 are comprised of the "base" requirements and additional requirements that are objective. The following table contains the "base" requirements that were validated as part of the Gossamer Security Solutions evaluation activities referenced above.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ALT_EXT.2: Agent Alerts	Samsung SDS EMM and EMM Agent for Android
	FAU_GEN.1(2): Audit Data Generation	Samsung SDS EMM and EMM Agent for Android
	FAU_SEL.1(2): Security Audit Event Selection	Samsung SDS EMM and EMM Agent for Android
FIA: Identification and Authentication	FIA_ENR_EXT.2: Agent Enrollment of Mobile Device into Management	Samsung SDS EMM and EMM Agent for Android
FMT: Security Management	FMT_POL_EXT.2: Agent Trusted Policy Update	Samsung SDS EMM and EMM Agent for Android
	FMT_SMF_EXT.4: Specification of Management Functions	Samsung SDS EMM and EMM Agent for Android
	FMT_UNR_EXT.1: User Unenrollment Prevention	Samsung SDS EMM and EMM Agent for Android

The following table contains requirements that only apply when the Module is paired with a certain Base-PP. If no completed evaluations have claimed a given requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "Module Evaluation."

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_STG_EXT.1(2): Cryptographic Key Storage	Samsung SDS EMM and EMM Agent for Android
	FCS_STG_EXT.4: Cryptographic Key Storage	Module Evaluation
FTP: Trusted Path/Channels	FTP_ITC_EXT.1(2): Trusted Channel Communication	Module Evaluation
	FTP_TRP.1(2): Trusted Path (for Enrollment)	Module Evaluation

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 ACE work units and has indicated its verification through "Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
The MOD_MDM_AGENT_V1.0 does not define any additional optional requirements.		

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 ACE work units and has indicated its verification through "Module Evaluation."

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
The MOD_MDM_AGENT_V1.0 does not define any additional selection-based requirements.		

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 ACE work units and has indicated its verification through "Module Evaluation."

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG_EXT.3: Security Audit Event Storage	Module Evaluation
FPT: Protection of the TSF	FPT_NET_EXT.1: Network Reachability	Module Evaluation

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_MDM_V4.0. The SARs defined in that PP are applicable to MOD_MDM_AGENT_V1.0 as well as CFG_MDM-MDM_AGENT_V1.0 as a whole.

7 Results of the Evaluation

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

Table 11: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module evaluation
ACE_CCL.1	Pass	Module evaluation
ACE_SPD.1	Pass	Module evaluation
ACE_OBJ.1	Pass	Module evaluation
ACE_ECD.1	Pass	Module evaluation
ACE_REQ.1	Pass	Module evaluation
ACE_MCO.1	Pass	Module evaluation
ACE_CCO.1	Pass	Module 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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_MDM_AGENT_V1.0 Evaluation Activities to determine whether 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 the CCEVS Validation Body uses that leads to the issuance 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 Organizations. *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 Organizations. *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 Organizations. *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 Organizations. *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] PP-Module for MDM Agents, Version 1.0, 25 April 2019.

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

[8] PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, 27 January 2020.

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

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