National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Mobile Device Management, Version 1.1, March 7th, 2014

Report Number: CCEVS-VR-PP-0015
Dated: 27 October 2015
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 Inc.
Catonsville, Maryland

Table of Contents

List of Tables

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 1.1 (MDMPP11). It presents a summary of the MDMPP11 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the MDMPP11 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Samsung SDS Co., LTD Samsung SDS CellWe EMM version 1.1. The evaluation was performed by the Gossamer Security Solutions Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in May 2015. This evaluation addressed the base requirements of the MDMPP.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the Gossamer Security Solutions Inc. CCTL.

The evaluation determined that the MDMPP11 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP 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). The ST contains material drawn directly from the MDMPP11.

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

The validation team found that the evaluation showed that the MDMPP11 meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

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). CCTLs evaluate products against Protection Profile containing Assurance 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 the MDMPP11 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Samsung SDS Co., Samsung SDS CellWe EMM version 1.1., developed by Samsung SDS Co., LTD. The evaluation was performed by the Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in May 2015.

The MDMPP11 contains a set of "base" requirements that all conformant STs must include and "additional" requirements that may or may not apply to a conformant TOE depending on its architecture and intended usage.

Because these optional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the MDMPP11 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the MDMPP11.

Protection Profile	*Protection Profile for Mobile Device Management,, Version 1.1*
ST (Base)	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
Evaluation Technical Report (Base)	Evaluation Technical Report for Samsung SDS Co. Ltd EMM Suite (MDMPP11), Version 1.3, April 18, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base)	Gossamer Security Solutions, Catonsville, MD USA
CCEVS Validators (base)	Kenneth Elliott, Aerospace Corporation
	Jerome Myers, Aerospace Corporation
	Ken Stutterheim, Aerospace Corporation
	Sheldon Durrant, Mitre Corporation

3 MDMPP Description

Mobile device management (MDM) products allow enterprises to apply security policies to mobile devices, such as smartphones and tablets. The purpose of these policies is to establish a security posture adequate to permit mobile devices to process enterprise data and connect to enterprise network resources.

This document provides a baseline set of Security Functional Requirements (SFRs) for an MDM system, which is the Target of Evaluation (TOE). The MDM system is only one component of an enterprise deployment of mobile devices. Other components, such as the mobile device platforms which enforce the security policies, and servers which host mobile application repositories, are out of scope.

4 Security Problem Description and Objectives

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: TOE Assumptions

Assumption Name	Assumption Definition
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 an evaluated Mobile platform and hardware to provide policy enforcement as well as cryptographic services and data protection.
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 logon services via a local or network directory service, and to provide basic audit log management functions. 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_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.

Threats

The following threats should be integrated into the threats that are specific to the technology by the ST authors when including the requirements described in this document. Modifications, omissions, and additions to the requirements may impact this list, so the ST author should modify or delete these threats as appropriate.

Table 2: Threats

Threat Name	Threat Definition
T.MALICIOUS_APPS	An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE or OE, resulting in the compromise of TOE or TOE data.
T.NETWORK_ATTACK	An attacker may masquerade as MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands. An attacker may masquerade as MDM Agent and attempt to compromise the integrity of the MDM by sending malicious records.

Threat Name	Threat Definition
T.NETWORK_EAVESDROP	Unauthorized entities may intercept communications between the MDM and mobile devices to monitor, gain access to, disclose, or alter remote management commands. Unauthorized entities may intercept unprotected wireless communications between the mobile device and the Enterprise to monitor, gain access to, disclose, or alter TOE data.
T.PHYSICAL_ACCESS	The mobile device may be lost or stolen, and an unauthorized individual may attempt to access OE data.

Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following OSPs must be enforced by the TOE or its operational environment.

Table 3: Organizational Security Policies

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 84 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 mobile device is lost or stolen.
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.

Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the mobile OS. This will include the initial enrollment of the device into management, through its lifecycle including policy updates and through its possible unenrollment from management services.
O.ACCOUNTABILITY	The TOE must provide logging facilities which record management actions undertaken by its administrators
O.DATA_PROTECTION_TRANSIT	Data exchanged between and from elements of the TOE and its operating environment must be protected from being monitored, accessed and altered.
O.MANAGEMENT	The TOE provides access controls around its management functionality.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
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 85 cryptographic services and data protection.
OE.MDM_SERVER_PLATFORM	The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities.
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.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.
OE.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.

5 Requirements

As indicated above, requirements in the MDMPP11 are comprised of the "base" requirements and additional requirements that are conditionally or strictly optional. The following are table contains the "base" requirements that were validated as part of the CA evaluation activity referenced above.

TOE Security Functional Requirements

This section identifies the SFRs for the TOE.

Table 6: TOE Security Requirements

Requirement Class	Requirement Component
FAU: Security Audit	FAU_ALT_EXT.1: Agent Alerts
	FAU_ALT_EXT.2: Server Alerts
	FAU_GEN.1(1): Audit Data Generation (MDM Server
FIA: Identification and Authentication	FIA_ENR_EXT.1: Enrollment of Mobile Device into Management
FMT: Security Management	FMT_MOF.1(1): Management of functions in MDM Server
	FMT_MOF.1(2): Management of Enrollment Function
	FMT_POL_EXT.1 Trusted Policy Update (MDM Agent)
	FMT_SMF.1(1): Specification of management functions (Server configuration of Agent)
	FMT_SMF.1(2): Specification of management functions (Agent configuration of platform)
	FMT_SMF.1(3): Specification of management functions (Server Configuration of Server)

Requirement Class	Requirement Component
	FMT_SMR.1: Security Management Roles
FPT: Protection of the TSF	FPT_ITT.1: Basic Internal TSF Data Transfer Protection
	FPT_TUD_EXT.1(1): Trusted Update (MDM Server)
FTA: TOE Access	FTA_TAB.1: TOE Access Banner
FTP: Trusted Path/Channels	FTP_ITC.1(1): Inter-TSF Trusted Channel
	FTP_ITC.1(2): Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

MDM Server or Platform Security Functional Requirements

This section identifies the SFRs that must be performed by the MDM Server or by the MDM Server's platform. Each requirement includes a selection for the ST author to indicate whether the MDM Server or the MDM Server's platform performs the functionality in the requirement. The assurance activity for those requirements for which the platform has been selected is to verify that the platforms identified by the ST author are Common Criteria validated and to ensure that the ST for the platform includes the functionality in the requirement.

Table 7: MDM Server or Platform Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1(1): Audit Data Generation (MDM Server)
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic Support	FCS_CKM.1(1): Cryptographic Key Generation
	FCS_CKM.2(1): Cryptographic Key Storage (MDM Server)
	FCS_CKM_EXT.4(1): Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic Operation (Digital Signature)
	FCS_COP.1(2): Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_COP.1(3): Cryptographic Operation (Encryption and Decryption)
	FCS_COP.1(4): Cryptographic Operation (Hashing)
	FCS_RBG_EXT.1(1): Random Bit Generation
FIA: Identification and Authentication	FIA_UAU.1: Timing of Authentication
	FIA_X509_EXT.1(1): X509 Validation
	FIA_X509_EXT.2(1): X509 Authentication
FPT: Protection of the TSF	FPT_TST_EXT.1(1): TSF Testing
	FPT_TUD_EXT.1(1): Trusted Update (MDM Server)
FTP: Trusted Path/Channels	FTP_TRP.1: Trusted path for Remote Administration
	FTP_TRP.2: Trusted path for Enrollment
	FTA_SSL.4: User-initiated Termination
	FTA_TSE.1: TOE Session Establishment

MDM Agent or Platform Security Functional Requirements

This section identifies the SFRs that must be performed by the MDM Agent or by the MDM Agent's platform. Each requirement includes a selection for the ST author to indicate whether the MDM Agent or the MDM Agent's platform performs the functionality in the requirement. The assurance activity for those requirements for which the platform has been selected is to verify that the platforms identified by the ST author are Common Criteria validated and to ensure that the ST for the platform includes the functionality in the requirement.

Table 8: MDM Agent or Platform Security Functional Requirements

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_CKM.1(3): Cryptographic Key Generation
	FCS_CKM.2(2): Cryptographic Key Storage (MDM Agent)
	FCS_CKM_EXT.4(2): Cryptographic Key Destruction
	FCS_COP.1(5): Cryptographic Operation (Digital Signature)
	FCS_COP.1(6): Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_COP.1(7): Cryptographic Operation (Encryption and Decryption)
	FCS_COP.1(8): Cryptographic Operation (Hashing)
	FCS_RBG_EXT.1(2): Random Bit Generation
FIA: Identification and Authentication	FIA_X509_EXT.1(2): X509 Validation
	FIA_X509_EXT.2(2): X509 Authentication
FPT: Protection of the TSF	FPT_TST_EXT.1(2): TSF Testing

Additional Requirements

The following table contains the optional requirements contained in the appendices of the MDMPP11, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

5.1.1 Optional Requirements

Table 9: Optional TSF Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SEL.1(1): Security Audit Event Selection (MDM Server)	
	FAU_SAR.1: Audit Review (MDM Server)	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
	FAU_STG_EXT.2: Audit Event Storage	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015

5.1.2 Selection Based Requirements

Table 10: Selection Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_IV_EXT.1(1): Initialization Vector Generation	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
	FCS_STG_EXT.1 Encrypted Cryptographic Key Storage (MDM	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11)

Requirement Class	Requirement Component	Verified By
	Server)	Security Target, May 2015
	FCS_DTLS_EXT.1: DTLS Implementation	
	FCS_HTTPS_EXT.1: HTTPS Implementation	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
	FCS_IPSEC_EXT.1: Internet Protocol Security (IPsec) Communications	
	FCS_SSH_EXT.1: SSH Implementation	
	FCS_TLS_EXT.1: TLS Implementation	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
FIA: Identification and Authentication	FIA_X509_EXT.2(1): X509 Authentication	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
	FIA_X509_EXT.2(2): X509 Authentication	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015

5.1.3 Objective TSF Requirements

Table 11: Objective TSF Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1(2) Audit Data Generation (MDM Agent)	
	FAU_SEL.1(2) Security Audit Event Selection (MDM Agent)	
FCS: Cryptographic Support	FCS_CKM.1(4): Cryptographic Key Generation	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
FMT: Security Management	FMT_POL_EXT.1: Trusted Policy Update	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
	FIA_X509_EXT.2(2): X509 Authentication	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015
FTA: TOE Access	FTA_TAB.1: Default TOE Access Banners	Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target, May 2015

6 Assurance Requirements

The following are the assurance requirements contained in the MDMPP11:

Table 12: Security Assurance Requirements

Requirement Class	Requirement Component
ASE: Security Target	ASE_INT.1: ST Introduction
	ASE_CCL.1: Conformance Claims

	ASE_OBJ.1: Security Objectives for the Operational Environment
	ASE_ECD.1: Extended Components Definition
	ASE_REQ.1: Stated Security Requirements
	ASE_TSS.1: TOE Summary Specification
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE _ECD.1	Pass
APE _INT.1	Pass
APE _OBJ.2	Pass
APE _REQ.1	Pass

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 ESMACPP Assurance 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.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Gossamer Security Solutions Inc., *Samsung SDS Co., LTD Samsung SDS CellWe EMM (MDMPP11) Security Target*, Version 0.6, May 2015.

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

[8] Gossamer Security Solutions Inc., *Validation Report Samsung SDS Co, Ltd. Samsung SDS Co., LTD Samsung SDS CellWe EMM Suite*, Version 0.5, May 8th, 2015