BlackBerry Enterprise Service 12.5 Security Target

Doc No: 1958-002-D102
Version: 1.11
7 August 2018

BlackBerry
2200 University Ave. East
Waterloo, Ontario, Canada
N2K 0A7

Prepared by:
EWA-Canada
1223 Michael Street North
Ottawa, Ontario, Canada
K1J7T2

EWA CANADA | An Intertek Company

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the TOE, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and the Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.

Section 7, TOE Summary Specification, describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	BlackBerry Enterprise Service 12.5 Security Target
ST Version:	1.11
ST Date:	7 August 2018

1.3 TOE REFERENCE

TOE Name:	BlackBerry Enterprise Service
TOE Version:	Version 12.5.2 build 3.27.61

TOE Developer: BlackBerry

TOE Type: Mobile Device Management (MDM) Server

1.4 TOE OVERVIEW

BlackBerry Enterprise Service 12 (BES12) is an Enterprise Mobility Management solution from BlackBerry. It provides organizations with the ability to:

- Manage mobile devices for the organization to protect business information
- Maintain a connection to required information for mobile workers
- Provide administrators with efficient business tools to manage policy enforcement

BlackBerry 10 mobile devices, used with BES12, allow mobile workers secure access to mail, application and content servers in the organization's network, in accordance with the organization's policies. Evaluation of the BlackBerry 10 mobile device against the Protection Profile for Mobile Device Fundamentals and Extended Package for Mobile Device Management Agents has been performed in parallel with this evaluation. Figure 1 shows a TOE implementation scenario.

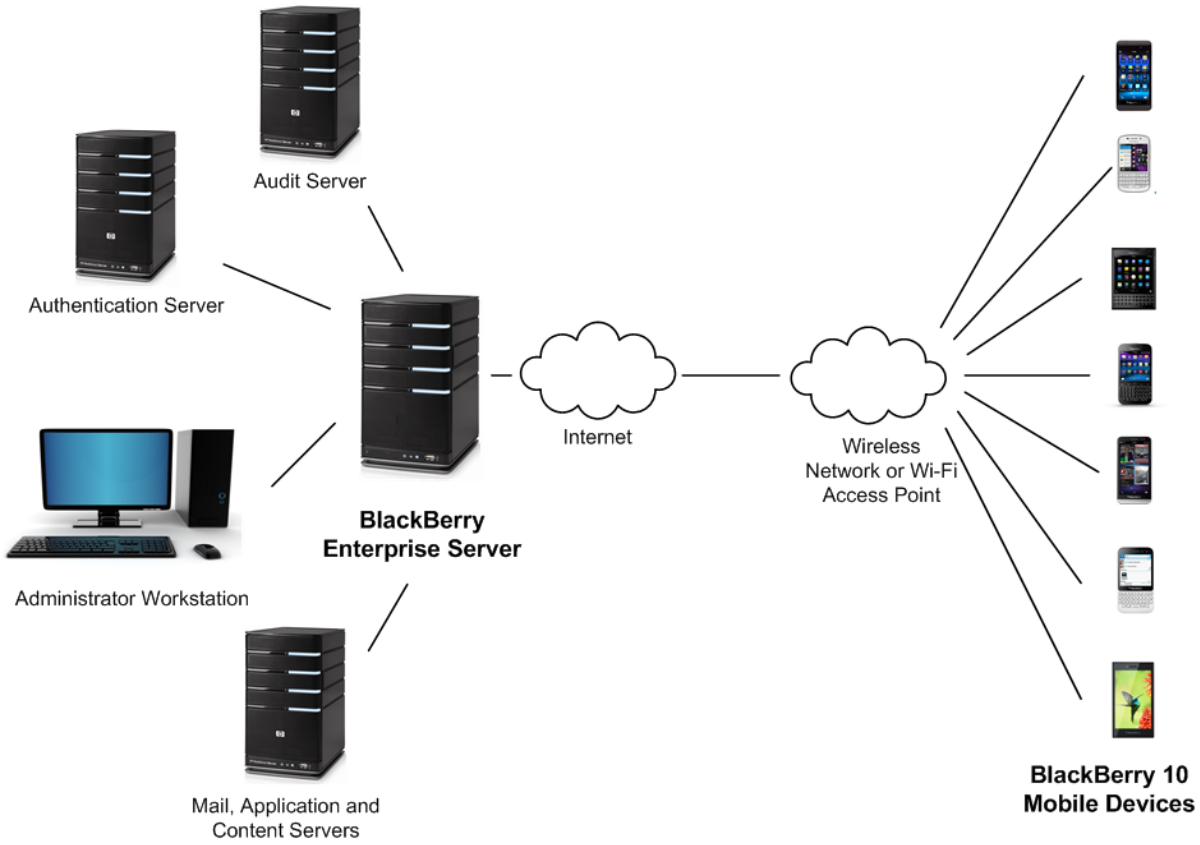

Figure 1 – BlackBerry Enterprise Service 12.5 Diagram

1.5 TOE AND TOE PLATFORM DESCRIPTION

1.5.1 Physical Scope

The Mobile Device Management system is the BES12 software running on Windows Server 2012 R2. Table 1 describes the TOE and the supported MDM Agents and MD platforms in the operational environment. Figure 2 shows the physical scope of the TOE.

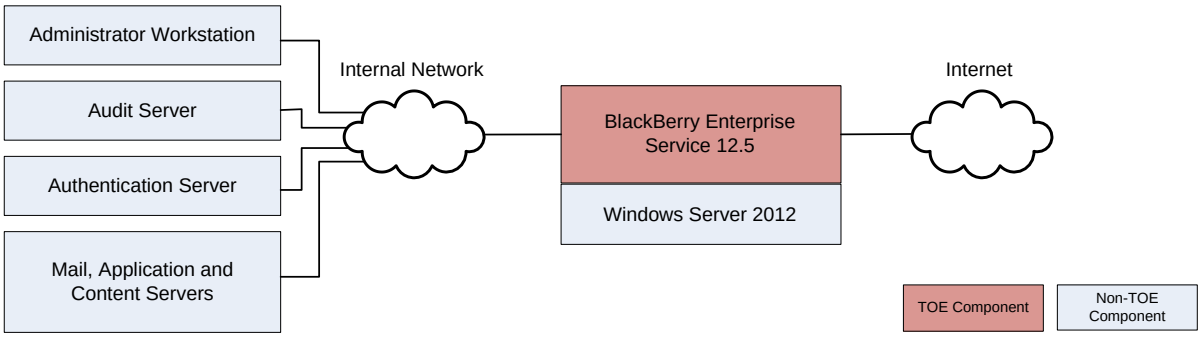

Figure 2 – TOE Boundary

Component	Location	Description
MDM Server (TOE)	TOE Component	The BlackBerry Enterprise Service 12.5 is the MDM Server. This includes the BlackBerry Resource Kit for BES 12 (Version 12.5.0 Bundle0008), the BES12 Configuration Tool (BES12ConfigTool.exe Version 1.25.7) and Validate Package (ValidatePackage.exe, Version 3.32.63). These files are not part of the primary installation package.
MDM Agent MDM Agent platform	Operational Environment	The BlackBerry 10 software on the BlackBerry 10 device (Passport, Classic, Leap, Z30, Z10, Q10, Q5 and P'9983) is the MDM Agent. It may be seen to be both the MDM Agent and the MDM Agent Platform as described in the MDM PP; however, the term MDM Agent is used in the Security Functional Requirements (SFRs).
MDM Server platform	Operational Environment	BlackBerry Enterprise Service 12.5 is supported by a Windows Server 2012 R2 platform, on general purpose computing hardware.
Audit Server	Operational Environment	In accordance with the requirements of the MDM PP, the TOE must be tested with an external audit server. A Windows Server 2012 R2 server was used for this evaluation.
Authentication Server	Operational Environment	The TOE has been tested with an external authentication server. Active Directory on a

Component	Location	Description
		Windows Server 2012 R2 server was used for this evaluation.
Administrator Workstation	Operational Environment	An administrator workstation is required to manage the BES12. For the purposes of the evaluation, a machine supporting Windows 10 was used.
BlackBerry Infrastructure	Operational Environment	The BlackBerry Infrastructure supports the use of 'push' technology on wireless carrier networks, minimizing the number of BES12 implementation connections that a carrier must support.

Table 1 – TOE and Operational Environment Components

1.5.2 TOE Platform Evaluation

The TOE Platform is Windows Server 2012 R2, referenced by Certification Report 2015-27-INF-1539v1. It is described in the Microsoft Windows Common Criteria Evaluation Microsoft Windows 10, Microsoft Windows Server 2012 R2 Security Target, dated March 17, 2016.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- Installation and Upgrade Guide BES12, Version 12.5 published 2016-06-30
- Configuration Guide BES12, Version 12.5, published 2017-01-27
- Administration Guide BES12, Version 12.5, published 2016-08-24
- Policy Reference Spreadsheet, BES12, Version 12.5, 2016-06-30
- BlackBerry Enterprise Service 12.5 Common Criteria Guidance Supplement, Version 1.0

1.5.4 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. The following breakdown also provides the description of the security features of the TOE, and loosely follows the security functional classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. Key events trigger an alert to the administrator. Administrators may verify the network connectivity status of an enrolled agent. Audit logs may be read from the MDM Server, and may be sent for external storage.

Functional Classes	Description
Cryptographic Support	Cryptographic functionality is provided in support of random bit and key generation, key distribution and establishment, key storage, key destruction and key operation for the TSF and the TOE platform. Specified cryptographic functions include the HTTPS and TLS protocols.
Identification and Authentication	Users must be authenticated prior to being allowed access to MDM Server functionality. Device enrollment is subject to policies. X.509 certificates must be used to support authentication and must be validated in accordance with policies.
Security Management	The TOE provides management capabilities covering device enrollment, policy update, server configuration of the agent, and server configuration of the server. Various roles are maintained.
Protection of the TSF	Self-tests must be run at start up. Trusted updates may be performed by authorized administrators.
TOE Access	A banner is presented on user login to the MDM Server.
Trusted Path/Channel	The communications links between the MDM Server and the audit server, between the MDM Server and the remote administrator, and between the MDM Server and the Mobile Device, including communications for enrollment activities, are protected using HTTPS (TLS).

Table 2 – Logical Scope of the TOE

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 [CEM] has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

This Security Target does not claim conformance to an Assurance Package, but conforms to the Security Assurance Requirements described in Section 5 of the Protection Profile for Mobile Device Management Version 2.0 dated 31 December 2014.

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

The Security Target claims exact conformance with the NIAP Protection Profile for Mobile Device Management Version 2.0 dated 31 December 2014. BES 12.5 is intended to address the security problems associated with the Enterprise-owned device for specialized, high-security use case. The following technical decisions have been considered: TD0034, TD0037, TD0040, TD0057, TD0078, TD0079, TD0082, TD0084, TD0107, TD0212 and TD 0234.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 3 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1 Security Objectives.

Threat	Description
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.
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.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. Table 4 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
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

OSP	Description
	actions via the MDM system.
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
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 the 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_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.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the MDM Agent. 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 the MDM Server and the MDM Agent and between the MDM Server and its operating environment must be protected from being monitored, accessed and altered.
O.MANAGEMENT	The TOE provides access controls around its management functionality.
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.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Table 7 identifies and describes the security objectives that are to be addressed by the IT domain or by non-technical or procedural means.

Security Objective	Description
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.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.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES CORRESPONDENCE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.MALICIOUS_APPS	T.NETWORK_ATTACK	T.NETWORK_EAVESDROP	T.PHYSICAL_ACCESS	P.ADMIN	P.DEVICE_ENROLL	P.NOTIFY	P.ACCOUNTABILITY	A.CONNECTIVITY	A.MDM_SERVER_PLATFORM	A.PROPER_ACMIN	A.PROPER_USER	A.ATIMESTAMP
O.APPLY_POLICY	X			X									
O.ACCOUNT-ABILITY								X					
O.DATA_ PROTECTION_ TRANSIT		X	X										
O.MANAGEMENT					X	X							
O.INTEGRITY	X												
OE.IT_ENTERPRISE						X							

	T.MALICIOUS_APPS	T.NETWORK_ATTACK	T.NETWORK_EAVESDROP	T.PHYSICAL_ACCESS	P.ADMIN	P.DEVICE_ENROLL	P.NOTIFY	P.ACCOUNTABILITY	A.CONNECTIVITY	A.MDM_SERVER_PLATFORM	A.PROPER_ACMIN	A.PROPER_USER	A.ATIMESTAMP
OE.MDM_SERVER_ PLATFORM										X			
OE.PROPER_ADMIN					X						X		
OE.PROPER_USER							X					X	
OE.WIRELESS_ NETWORK									X				
OE.TIMESTAMP										X			X

Table 8 – Mapping Between Objectives, Threats, OSPs, and Assumptions

5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFR)s used in this ST. The extended SFRs included in this ST originate from the Protection Profile for Mobile Device Management. The extended components are:

a. FAU_ALT_EXT.1 Server Alerts;
b. FAU_NET_EXT.1 Network Reachability Review;
c. FAU_STG_EXT.1 Extended: External audit trail storage;
d. FAU_STG_EXT.2 Audit Event Storage;
e. FCS_CKM_EXT.4 Cryptographic key Destruction;
f. FCS_HTTPS_EXT.1 HTTPS Protocol;
g. FCS_IV_EXT.1 Initialization Vector Generation;
h. FCS_RBG_EXT.1 Extended: Random Bit Generation;
i. FCS_STG_EXT.1 Cryptographic Key Storage;
j. FCS_STG_EXT.2 Encrypted Cryptographic Key Storage;
k. FCS_TLSC_EXT.1 TLS Protocol;
l. FCS_TLSS_EXT.1 TLS Server Protocol;
m. FIA_ENR_EXT.1 Enrollment of Mobile Device into Management;
n. FIA_X509_EXT.1 Validation of certificates;
o. FIA_X509_EXT.2 X509 Authentication;
p. FMT_POL_EXT.1 Trusted policy update;
q. FPT_TST_EXT.1 TSF testing; and
r. FPT_TUD_EXT.1 Trusted Update.

Dependency information for extended components may be found in the Protection Profile for Mobile Device Management and its annexes. Dependencies determined by selections are not included in the extended components definition.

5.1 CLASS FAU: SECURITY AUDIT

Three families have been added to the Security audit class. FAU_ALT_EXT deals with alerts and is modelled after the FAU_ARP Security audit automatic response family. FAU_ALT_EXT.1 is modelled after FAU_ARP.1 Security alarms. FAU_NET_EXT is used to make claims for support for verifying that an agent may be reached and is modelled after the FAU_ARP Security audit automatic response family. FAU_NET_EXT.1 is modelled after FAU_ARP.1 Security alarms. FAU_STG_EXT.1 and FAU_STG_EXT.2 are part of the Security audit event storage family, and are modelled after FAU_STG.2 Guarantees of audit data availability.

5.1.1 FAU_ALT_EXT

Family Behaviour

This family defines the requirements for providing alerts to the administrator.

Component Levelling

Figure 3 – FAU_ALT_EXT: Alerts Component Levelling

Management

There are no management activities foreseen.

Audit

Type of alert and the identity of the Mobile Device that sent the alert must be audited.

FAU_ALT_EXT.1 Server Alerts

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_ALT_EXT.1.1 The MDM Server shall alert the administrators in the event of any of the following:

a. change in enrollment status;

b. failure to apply policies to a mobile device;

c. [selection: [assignment: *other events*], no other events].

5.1.2 FAU_NET_EXT

Family Behaviour

This family defines the requirements for determining network connectivity status.

Component Levelling

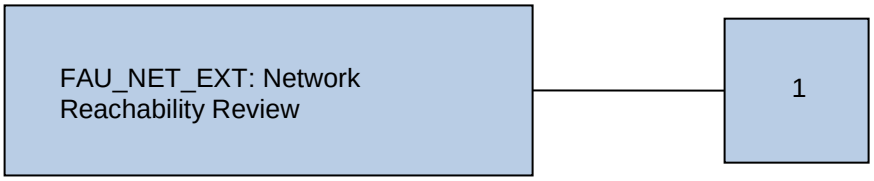

Figure 4 – FAU_NET_EXT: Network Reachability Review Component Levelling

Management

The security management function to query connectivity status is required.

Audit

There are no auditable events foreseen.

FAU_NET_EXT.1 Network Reachability Review

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_NET_EXT.1.1 The MDM Server shall provide authorized administrators with the capability to read the network connectivity status of an enrolled agent.

5.1.3 FAU_STG

Family Behaviour

This family defines the requirements for external audit trail storage.

Component Levelling

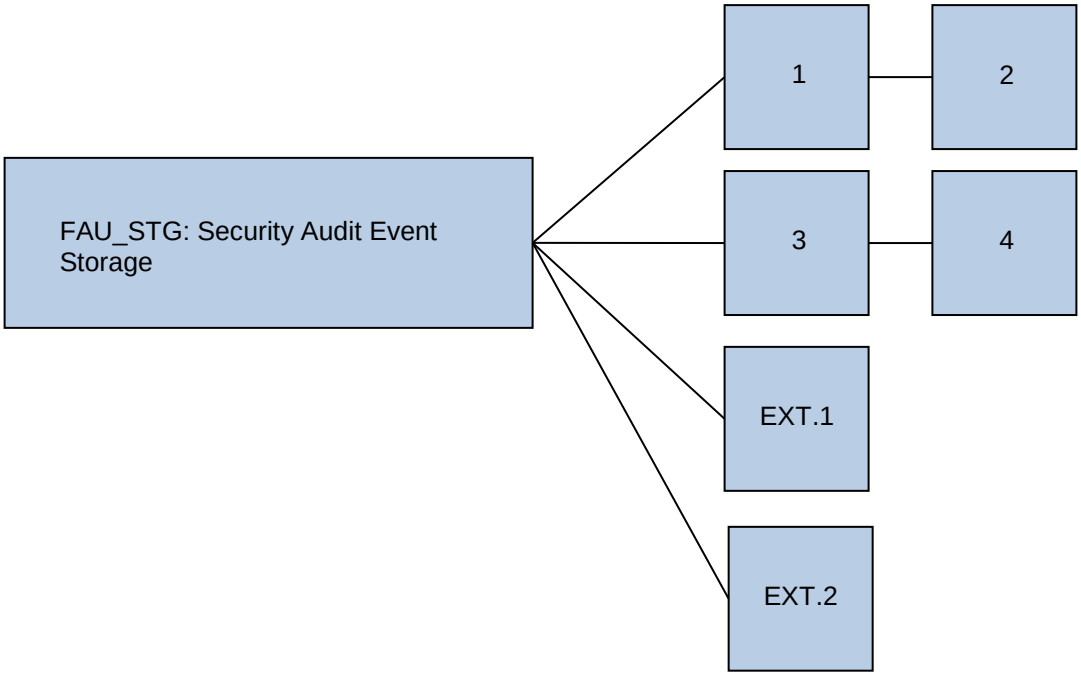

Figure 5 – FAU_STG: Security Audit Event Storage Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.1.1 The [selection: MDM Server, MDM Server platform] shall be able to transmit the generated audit data to an external IT entity using a trusted channel implementing the [selection: IPsec, SSH, TLS, TLS/HTTPS] protocol.

FAU_STG_EXT.2 Audit Event Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.2.1 The [selection: MDM Server, MDM Server platform] shall protect the stored audit records in the audit trail from unauthorized modification.

5.2 CLASS FCS: CRYPTOGRAPHIC SUPPORT

Six families have been added to the Cryptographic support class. FCS_HTTPS_EXT is modelled after FCS_COP Cryptographic operations, and FCS_HTTPS_EXT.1 is modelled after FCS_COP.1 Cryptographic key generation. FCS_IV_EXT is modelled after FCS_CKM Cryptographic key management, and FCS_IV_EXT.1 is modelled after FCS_CKM.1 Cryptographic key generation. FCS_RBG_EXT is modelled after FCS_CKM Cryptographic key management, and FCS_RBG_EXT.1 is modelled after FCS_CKM.1 Cryptographic key generation. FCS_STG_EXT is modelled after FCS_CKM Cryptographic key management, and FCS_STG_EXT.1 is modelled after FCS_CKM.1 Cryptographic key generation. FCS_TLSC_EXT is modelled after FCS_COP Cryptographic operations, and FCS_TLSC_EXT.1 is modelled after FCS_COP.1 Cryptographic key generation. FCS_TLSS_EXT is modelled after FCS_COP Cryptographic operations, and FCS_TLSS_EXT.1 is modelled after FCS_COP.1 Cryptographic key generation. FCS_CKM_EXT.4 is part of the Cryptographic key management family and is modelled after FCS_CKM.4.

5.2.1 FCS_CKM

Family Behaviour

This family defines the requirements for key management.

Component Levelling

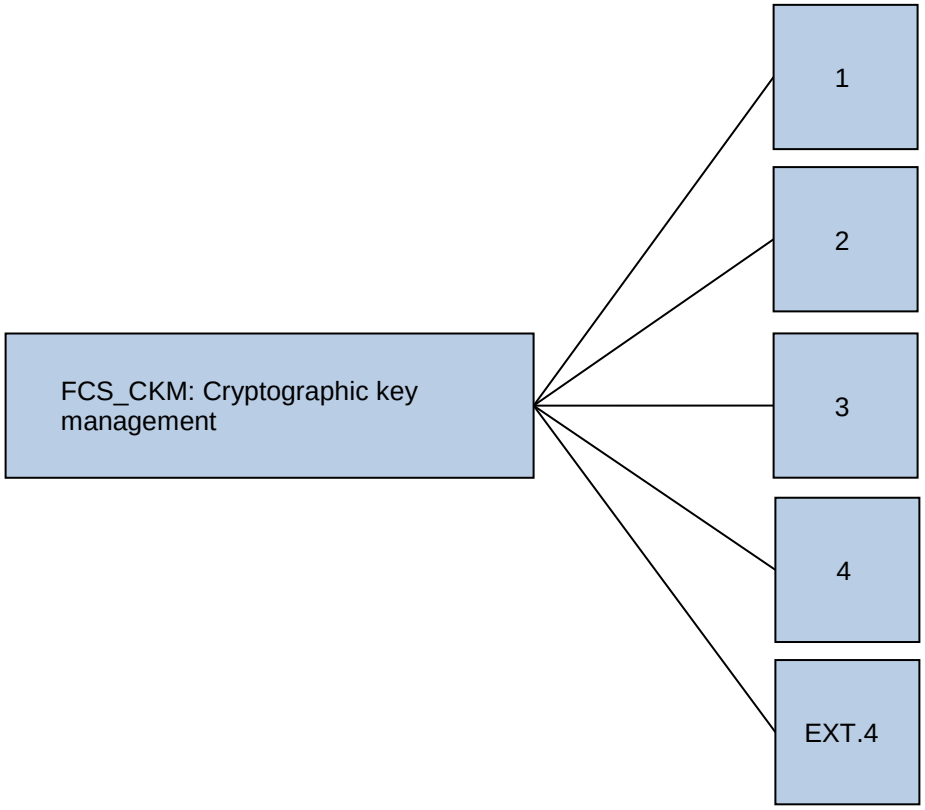

Figure 6 – FCS_CKM: Cryptographic Key Management Component Levelling

Management

The ability to destroy imported keys or secrets in the secure key storage may be required.

Audit

There are no auditable events foreseen.

FCS_CKM_EXT.4 Cryptographic Key Destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM_EXT.4.1 The TSF shall destroy cryptographic keys in accordance with the following rules:

- by clearing the KEK encrypting the target key,
- in accordance with the following rules:
  - For volatile memory, the destruction shall be executed by a single direct overwrite [selection: consisting of a pseudo-random pattern using the TSF's RBG, consisting of zeroes].
  - For non-volatile EEPROM, the destruction shall be executed by a single direct overwrite consisting of a pseudo random

pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), followed by a read-verify.

- o For non-volatile flash memory that is not wear leveled, the destruction shall be executed [selection: by a single direct overwrite consisting of zeros followed by a read-verify, by a block erase that erases the reference to memory that stores data as well as the data itself].
- o For non-volatile flash memory that is wear leveled, the destruction shall be executed [selection: by a single direct overwrite consisting of zeros, by a block erase].
- o For non-volatile memory other than EEPROM and flash, the destruction shall be executed by overwriting three or more times with a random pattern that is changed before each write.

FCS_CKM_EXT.4.2 The TSF shall destroy all plaintext keying material and critical security parameters (CSP) when no longer needed.

5.2.2 FCS_HTTPS_EXT

Family Behaviour

This family defines the requirements for support for the HTTPS protocol.

Component Levelling

Figure 7 – FCS_HTTPS_EXT: HTTPS Protocol Component Levelling

Management

The ability to configure X.509 certificates for MDM Server use is required.

Audit

Failure of the certificate validity check should be audited.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_HTTPS_EXT.1.1 The [selection: MDM Server, MDM Server platform] shall implement the HTTPS protocol that complies with RFC 2818.

FCS_ HTTPS_EXT.1.2 The [selection: MDM Server, MDM Server platform] shall implement HTTPS using TLS as specified in FCS_TLSS_EXT.1.

5.2.3 FCS_IV_EXT

Family Behaviour

This family defines the requirements for support for initialization vectors.

Component Levelling

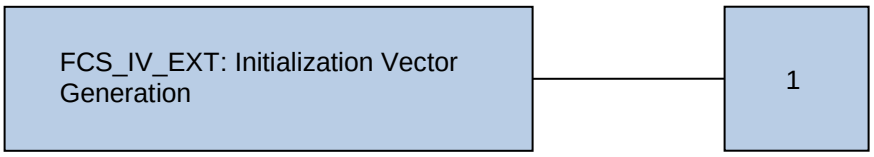

Figure 8 – FCS_IV_EXT: Initialization Vector Generation Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

FCS_IV_EXT.1 Initialization Vector Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_IV_EXT.1.1 The MDM Server shall generate IVs in accordance with Table 9.

Cipher Mode	Reference	IV Requirements
Electronic Codebook (ECB)	SP 800-38A	No IV
Counter (CTR)	SP 800-38A	"Initial Counter" shall be non-repeating. No counter value shall be repeated across multiple messages with the same secret key.
Cipher Block Chaining (CBC)	SP 800-38A	IVs shall be unpredictable. Repeating IVs leak information about whether the first one or more blocks are shared between two messages, so IVs should be non-repeating in such situations.
Output Feedback (OFB)	SP 800-38A	IVs shall be non-repeating and shall not be generated by invoking the cipher on another IV.
Cipher Feedback (CFB)	SP 800-38A	IVs should be non-repeating as repeating IVs leak information about the first plaintext block and about common shared prefixes in messages.
XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing (XTS)	SP 800-38E	No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer.
Cipher-based Message Authentication Code (CMAC)	SP 800-38B	No IV
Key Wrap and Key Wrap with Padding	SP 800-38F	No IV
Counter with CBC-	SP 800-38C	No IV. Nonces shall be non-repeating.

Cipher Mode	Reference	IV Requirements
Message Authentication Code (CCM)		
Galois Counter Mode (GCM)	SP 800-38D	IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key unless an implementation only uses 96-bit IVs (default length).

Table 9 – References and IV Requirements for NIST-approved Cipher Modes

5.2.4 FCS_RBG_EXT

Family Behaviour

This family defines the requirements for random bit generation.

Component Levelling

Figure 9 – FCS_RBG_EXT: Random Bit Generation Component Levelling

Management

There are no management activities foreseen.

Audit

Failure of the randomization process must be recorded.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The [selection: TSF, TOE platform] shall perform all deterministic random bit generation services in accordance with NIST Special Publication 800-90A using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: a software-based noise source, a platform-based RBG, a hardware-based noise source, no other sources] with a minimum of [selection: 128 bits, 256 bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

5.2.5 FCS_STG_EXT

Family Behaviour

This family defines the requirements for cryptographic key storage.

Component Levelling

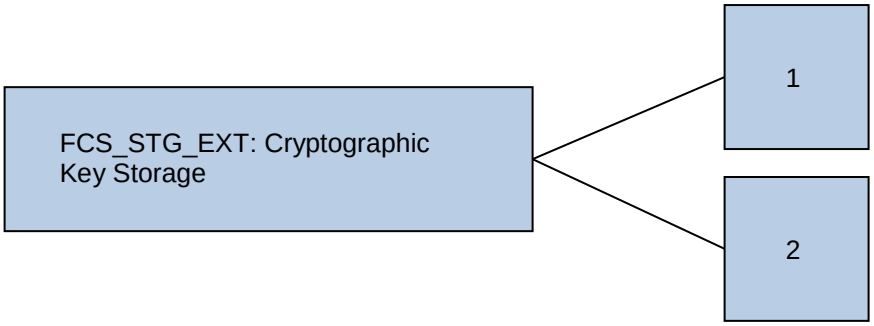

Figure 10 – FCS_STG_EXT: Cryptographic Key Storage Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

FCS_STG_EXT.1 Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_STG_EXT.1.1 The [selection: TSF, TOE platform] shall store persistent secrets and private keys when not in use, in [selection: platform-provided key storage, as specified in FCS_STG_EXT.2].

FCS_STG_EXT.2 Encrypted Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies: FCS_IV_EXT.1

FCS_STG_EXT.2.1 The MDM Server shall encrypt all keys using AES in the [selection: Key Wrap (KW) mode, Key Wrap with Padding (KWP) mode, GCM, CCM, CBC mode].

5.2.6 FCS_TLSC_EXT

Family Behaviour

This family defines the requirements for the TOE acting as a TLS Client.

Component Levelling

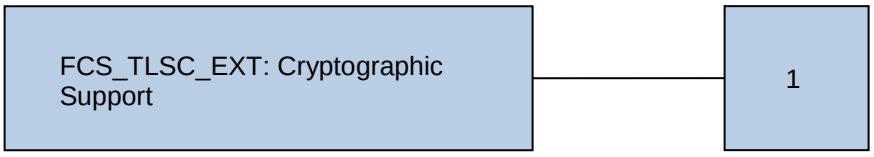

Figure 11 – FCS_TLSC_EXT: Cryptographic Support Component Levelling

Management

The ability to configure X.509 certificates for MDM Server use is required.

Audit

Failure to establish a TLS session, including reason for failure must be recorded. Failure to verify presented identifier must also be recorded.

FCS_TLSC_EXT.1 Cryptographic Support

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_TLSC_EXT.1.1 The [selection: TSF, TOE platform] shall implement [selection: TLS 1.0 (RFC 3246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- [Optional Ciphersuites:
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
  - no other ciphersuite]].

FCS_TLSC_EXT.1.2 The [selection: TSF, TOE platform] shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The [selection: TSF, TOE platform] shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.1.4 The [selection: TSF, TOE platform] shall support mutual authentication using X.509v3 certificates.

FCS_TLSC_EXT.1.5 The [selection: TSF, TOE platform] shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST

curves: [selection: secp256r1, secp384r1, secp521r1] and no other curves.

5.2.7 FCS_TLSS_EXT

Family Behaviour

This family defines the requirements for the TOE acting as a TLS Server.

Component Levelling

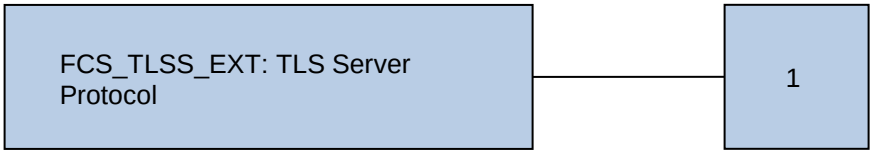

Figure 12 – FCS_TLSS_EXT: Cryptographic Support Component Levelling

Management

The ability to configure X.509 certificates for MDM Server use is required.

Audit

Failure to establish a TLS session, including reason for failure must be recorded.

FCS_TLSS_EXT.1 TLS Server Protocol

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_TLSS_EXT.1.1 The [selection: MDM Server, MDM Server platform] shall implement [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- [Optional Ciphersuites:
  - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- no other ciphersuite]].

FCS_TLSS_EXT.1.2 The [selection: MDM Server, MDM Server platform] shall deny connections from clients requesting SSL 1.0, SSL 2.0, SSL 3.0 and [selection: TLS 1.0, TLS 1.1, no other TLS version].

FCS_TLSS_EXT.1.3 The [selection: MDM Server, MDM Server platform] shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.1.4 The [selection: MDM Server, MDM Server platform] shall not establish a trusted channel if the peer certificate is invalid.

FCS_TLSS_EXT.1.5 The [selection: MDM Server, MDM Server platform] shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the peer.

FCS_TLSS_EXT.1.6 The [selection: MDM Server, MDM Server platform] shall generate key agreement parameters [selection: over NIST curves [selection: secp256r1, secp384r1] and no other curves; Diffie- Hellman parameters of size 2048 bits and [selection: 3072 bits, no other size]].

5.3 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

Two families have been added to the Identification and Authentication class. FIA_ENR_EXT is modelled after FIA_UAU User Authentication. FIA_ENR_EXT.1 Extended: Enrollment of Mobile Devices into Management is modelled after FIA_UAU.2 User authentication before any action. FIA_X509_EXT is modelled after FIA_UAU User Authentication. FIA_X509_EXT.1 X509 Validation and FIA_X509_EXT.2 X509 Authentication are both modelled after FIA_UAU.2 User authentication before any action.

5.3.1 FIA_ENR_EXT

Family Behaviour

This family defines the requirements for enrolling mobile devices into management.

Component Levelling

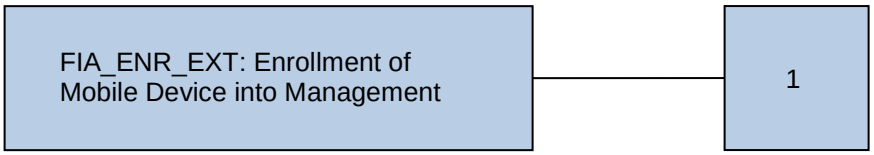

Figure 13 – FIA_ENR_EXT: Enrollment of Mobile Device into Management Component Levelling

Management

The ability to select devices for enrollment and unenrollment is required.

Audit

Failure of the Mobile Device user authentication, including the credentials presented, must be recorded.

FIA_ENR_EXT.1 Extended: Enrollment of Mobile Device into Management

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ENR_EXT.1.1 The MDM Server shall authenticate the remote user over a trusted channel during the enrollment of a mobile device.

FIA_ENR_EXT.1.2 The MDM Server shall limit the user's enrollment of devices to [selection: specific devices, specific device models, a number of devices, specific time period].

5.3.2 FIA_X509_EXT

Family Behaviour

This family defines the requirements for the validation of X.509 certificates, and the use of X.509 certificates in authentication.

Component Levelling

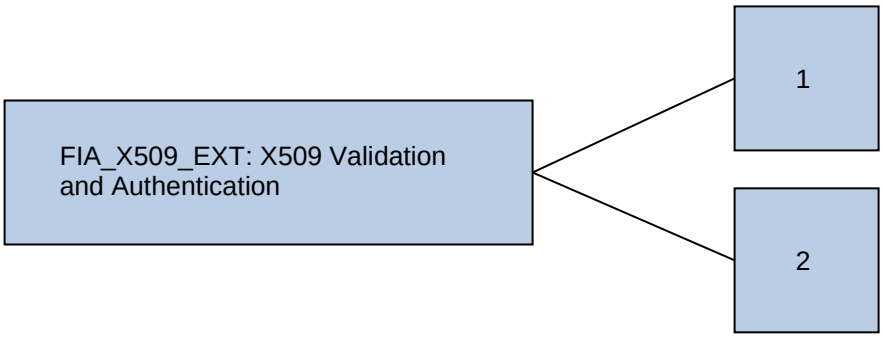

Figure 14 – FIA_X509_EXT: X509 Validation and Authentication Component Levelling

Management

There are no management activities foreseen.

Audit

For FIA_X509_EXT.1, failure of the X.509 certificate validation, including the reason for failure, must be recorded. For FIA_X509_EXT.2, failure to establish a connection to determine revocation status must be recorded.

FIA_X509_EXT.1 X509 Validation

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_X509_EXT.1.1 The [selection: TSF, TOE platform] shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - o Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

FIA_X509_EXT.1.2 The [selection: TSF, TOE platform] shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X509 Authentication

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1

FIA_X509_EXT.2.1 The [selection: TSF, TOE platform] shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: IPsec, TLS, HTTPS, DTLS]], and [selection: code signing for system software updates, code signing for integrity verification, policy signing, no additional uses].

FIA_X509_EXT.2.2 When the [selection: TSF, TOE platform] cannot establish a connection to determine the validity of a certificate, the [selection:

TSF, TOE platform] shall [selection: allow the administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate].

FIA_X509_EXT.2.3 The [selection: TSF, TOE platform] shall require a unique certificate for each client device.

5.4 CLASS FMT: SECURITY MANAGEMENT

A new family has been added to the Security management class. FMT_POL_EXT allows for policy updates and is modelled after the FMT_MTD Management of TSF data family. FMT_POL_EXT.1 is modelled after FMT_MTD.1 Management of TSF data.

5.4.1 FMT_POL_EXT

Family Behaviour

This family defines the requirements for providing trusted policy updates from the MDM server to the mobile device.

Component Levelling

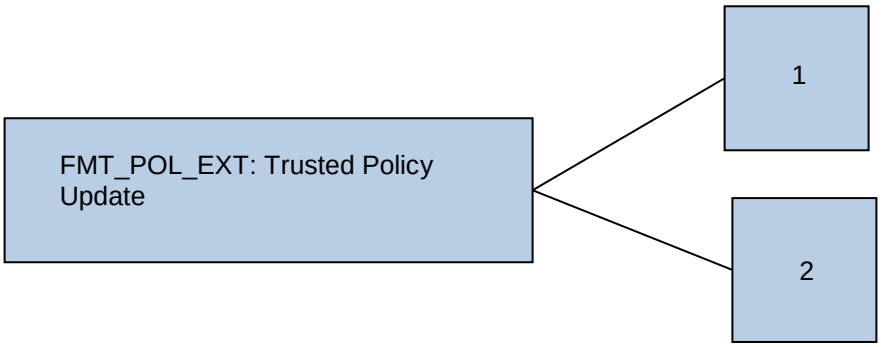

Figure 15 – FMT_POL_EXT: Trusted Policy Update Component Levelling

Management

Management functionality to set and deliver policy information is required.

Audit

There are no auditable events foreseen.

FMT_POL_EXT.1 Trusted Policy Update

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_POL_EXT.1.1 The MDM Server shall provide digitally signed policies and policy updates to the MDM Agent.

5.5 CLASS FPT: PROTECTION OF THE TSF

A new family has been added to the Protection of the TSF class. FPT_TUD_EXT addresses updates. FPT_TUD_EXT is modelled after the FPT_SSP State synchrony protocol family, and FPT_TUD_EXT.1 is modelled after FPT_SSP.1 Simple trusted acknowledgement. An extended SFR has been added to the TSF self test family to address TOE-specific TSF self tests.

5.5.1 FPT_TST

Family Behaviour

This family defines the requirements for the self testing of the TSF.

Component Levelling

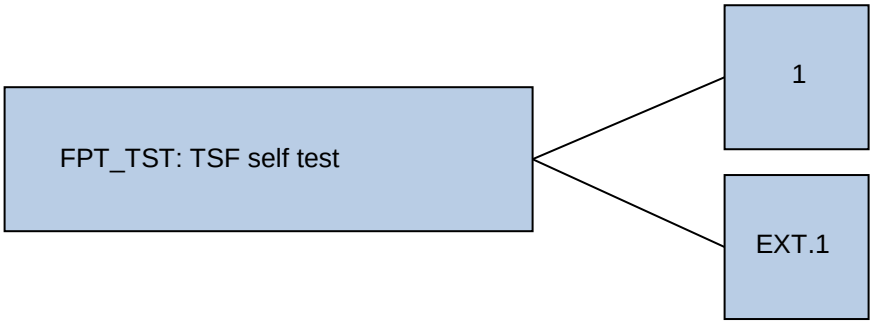

Figure 16 – FPT_TST: TSF self test Component Levelling

Management FPT_TST_EXT.1

There are no management activities foreseen.

Audit FPT_TST_EXT.1

Initiation of the self-test, failure of the self-test (with the algorithm that caused the failure) and detected integrity violations (with the code file that caused the integrity violation) must be recorded.

FPT_TST_EXT.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The [selection: MDM Server, MDM Server platform] shall run a suite of self tests during initial start-up (on power on) to demonstrate correct operation of the TSF.

FPT_TST_EXT.1.2 The [selection: MDM Server, MDM Server platform] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the [selection: TSF, TOE platform]-provided cryptographic services.

5.5.2 FPT_TUD_EXT

Family Behaviour

This family defines the requirements for trusted update.

Component Levelling

Figure 17 – FPT_TUD_EXT: Extended: Trusted Update Component Levelling

Management

There are no management activities foreseen beyond those described in the FPT_TUD_EXT.1.

Audit FPT_TUD_EXT.1

Success or failure of the signature verification must be recorded.

FPT_TUD_EXT.1 Extended: Trusted Update

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TUD_EXT.1.1 The MDM Server shall provide Authorized Administrators the ability to query the current version of the MDM Server software.

FPT_TUD_EXT.1.2 The [selection: MDM Server, MDM Server platform] shall provide Authorized Administrators the ability to initiate updates to TSF software.

FPT_TUD_EXT.1.3 The [selection: MDM Server, MDM Server platform] shall provide a means to verify software updates to the TSF using a digital signature mechanism prior to installing those updates.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and extended requirements, as described in the Protection Profile for Mobile Device Management.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the manner used in the Protection Profile.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_ALT_EXT.1	Server Alerts
	FAU_GEN.1(1)	Audit data generation (MDM Server)
	FAU_NET_EXT.1	Network Reachability Review
	FAU_SAR.1	Audit review
	FAU_STG_EXT.1	Extended: External audit trail storage
	FAU_STG_EXT.2	Audit Event Storage
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution/establishment
	FCS_CKM_EXT.4	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic operation (Confidentiality Algorithms)
	FCS_COP.1(2)	Cryptographic operation (Hashing)
	FCS_COP.1(3)	Cryptographic operation (Digital Signature)
	FCS_COP.1(4)	Cryptographic operation (Keyed-Hash Message Authentication)
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_IV_EXT.1	Initialization Vector Generation

Class	Identifier	Name
	FCS_RBG_EXT.1	Extended: Random Bit Generation
	FCS_STG_EXT.1	Cryptographic Key Storage
	FCS_STG_EXT.2	Encrypted Cryptographic Key Storage
	FCS_TLSC_EXT.1	Cryptographic Support
	FCS_TLSS_EXT.1	TLS Server Protocol
Identification and Authentication (FIA)	FIA_ENR_EXT.1	Enrollment of Mobile Device into Management
	FIA_UAU.1	Timing of authentication
	FIA_X509_EXT.1	Validation of certificates
	FIA_X509_EXT.2	X509 Authentication
Security Management (FMT)	FMT_MOF.1(1)	Management of security functions behaviour (Management of Functions in MDM Server)
	FMT_MOF.1(2)	Management of security functions behaviour (Management of Enrollment function)
	FMT_POL_EXT.1	Trusted policy update
	FMT_SMF.1(1)	Specification of Management Functions (Server configuration of Agent)
	FMT_SMF.1(2)	Specification of Management Functions (Server Configuration of Server)
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_TST_EXT.1	TSF testing
	FPT_TUD_EXT.1	Trusted Update
TOE Access	FTA_TAB.1	Default TOE access banners
Trusted path/channels (FTP)	FTP_ITC.1(1)	Inter-TSF Trusted channel (Authorized IT Entities) (MDM Server)
	FTP_ITC.1(2)	Inter-TSF Trusted channel (MDM Agent)
	FTP_TRP.1(1)	Trusted Path for Remote Administration
	FTP_TRP.1(2)	Trusted Path for Enrollment

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_ALT_EXT.1 Server Alerts

FAU_ALT_EXT.1.1 The MDM Server shall alert the administrators in the event of any of the following:

a. change in enrollment status;

b. failure to apply policies to a mobile device;

c. [no other events].

6.2.1.2 FAU_GEN.1(1) Audit data generation (MDM Server)

FAU_GEN.1.1(1)Refinement: The **MDM Server** shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the MDM Server software;

b. All administrative actions;

c. Commands issued from the MDM Server to an MDM Agent;

d. Specifically defined auditable events listed in Table 11.

FAU_GEN.1.2(1) Refinement: The [*MDM Server, MDM Server Platform*] shall record within each TSF audit record at least the following information:

- date and time of the event,
- type of event,
- subject identity,
- (if relevant) the outcome (success or failure) of the event,
- additional information in Table 11,
- [*no other audit relevant information*].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ALT_EXT.1	Type of alert.	Identity of Mobile Device that sent alert.
FAU_GEN.1(1)	None.	
FAU_NET_EXT.1	None.	
FAU_SAR.1	None.	
FAU_STG_EXT.1	None.	
FAU_STG_EXT.2	None.	
FCS_CKM_EXT.4	None.	
FCS_CKM.1	Failure of the key generation activity for authentication keys.	No additional information.
FCS_CKM.2	None.	

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_HTTPS_EXT.1	Failure of the certificate validity check.	
FCS_IV_EXT.1	None.	
FCS_RBG_EXT.1	Failure of the randomization process.	No additional information.
FCS_STG_EXT.1	None.	
FCS_STG_EXT.2	None.	
FCS_TLSC_EXT.1	Failure to establish a TLS session. Failure to verify presented identifier.	Reason for failure. Presented identifier and reference identifier.
FCS_TLSS_EXT.1	Failure to establish a TLS session.	Reason for failure.
FIA_ENR_EXT.1	Failure of MD user authentication.	Presented credentials.
FIA_UAU.1	None.	
FIA_X509_EXT.1	Failure of X.509 certificate validation.	Reason for failure of validation.
FIA_X509_EXT.2	Failure to establish connection to determine revocation status[1].	No additional information.
FMT_MOF.1(1)	Issuance of command to perform function. Change of policy settings.	Command sent and identity of MDM Agent recipient. Policy changed and value or full policy.
FMT_MOF.1(2)	Enrollment by a user	Identity of user.
FMT_POL_EXT.1	None.	

[1] BES 12 provides its own Certification Authority through the CORE service, which determines certificate revocation status from an internal database. If the database is unavailable, the CORE service cannot function. Audit records will show failures, but not specifically show a failure to establish a connection for the purposes of determining revocation status.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMF.1(1)	None.	
FMT_SMF.1(2)	Success or failure of function.	No additional information.
FMT_SMR.1	None.	
FPT_TST_EXT.1	Initiation of self-test. Failure of self-test. Detected integrity violation.	Algorithm that caused failure. The TSF code file that caused the integrity violation.
FPT_TUD_EXT.1	Success or failure of signature verification.	
FTA_TAB.1	Change in banner setting.	No additional information.
FTP_ITC.1(1)	Initiation and termination of the trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.
FTP_ITC.1(2)	Initiation and termination of the trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.
FTP_TRP.1(1)	Initiation and termination of the trusted channel.	Trusted channel protocol. Identity of the administrator.
FTP_TRP.1(2)	Initiation and termination of the trusted channel.	Trusted channel protocol.

Table 11 – TOE Security Functional Requirements and Auditable Events - Server

6.2.1.3 FAU_NET_EXT.1 Network Reachability Review

FAU_NET_EXT.1.1 The MDM Server shall provide authorized administrators with the capability to read the network connectivity status of an enrolled agent.

6.2.1.4 FAU_SAR.1 Audit review

FAU_SAR.1.1 Refinement: The **[MDM Server]** shall provide **Authorized Administrators** with the capability to read **all audit data** from the audit records.

FAU_SAR.1.2 Refinement: The **[MDM Server]** shall provide the audit records in a manner suitable for the Authorized Administrators to interpret the information.

6.2.1.5 FAU_STG_EXT.1 Extended: External audit trail storage

FAU_STG_EXT.1.1 The [MDM Server] shall be able to transmit audit data to an external IT entity using a trusted channel implementing the [TLS/HTTPS] protocol.

6.2.1.6 FAU_STG_EXT.2 Audit Event Storage

FAU_STG_EXT.2.1 The [MDM Server platform] shall protect the stored audit records in the audit trail from unauthorized modification.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 Refinement: The **[TSF]** shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- **RSA schemes using** cryptographic key sizes of **2048-bit or greater** that meet the following: [
  - **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3]**;
- **ECC schemes using "NIST curves" P-384 and [P-256, P-521]** that meet the following: **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;**
- **FFC schemes using** cryptographic key sizes of **2048-bit or greater** that meet the following: **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1**

].

6.2.2.2 FCS_CKM.2 Cryptographic key distribution / establishment (TSF)

FCS_CKM.2.1 Refinement: The [**TSF**] shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- **RSA-based key establishment schemes** that meets the following: **NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"**;
- **Elliptic curve-based key establishment schemes** that meets the following: **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**;
- **Finite field-based key establishment schemes** that meets the following: **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**;

].

6.2.2.3 FCS_CKM_EXT.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy cryptographic keys in accordance with the specified cryptographic key destruction methods:

- by clearing the KEK encrypting the target key,
- in accordance with the following rules:
  - For volatile memory, the destruction shall be executed by a single direct overwrite [consisting of zeroes].
  - For non-volatile EEPROM, the destruction shall be executed by a single direct overwrite consisting of a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), followed by a read-verify.

- o For non-volatile flash memory that is not wear-leveled, the destruction shall be executed [by a single direct overwrite consisting of zeros followed by a read-verify].
- o For non-volatile flash memory that is wear-leveled, the destruction shall be executed [by a single direct overwrite consisting of zeros].
- o For non-volatile memory other than EEPROM and flash, the destruction shall be executed by overwriting three or more times with a random pattern that is changed before each write.

FCS_CKM_EXT.4.2 The TSF shall destroy all plaintext keying material and critical security parameters (CSP) when no longer needed.

Application Note: The TSF does not store plaintext keying material or critical security parameters in non-volatile flash memory. The selection is made for completeness.

6.2.2.4 FCS_COP.1(1) Cryptographic operation (Confidentiality Algorithms)

FCS_COP.1.1(1) Refinement: The **[TSF]** shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm [

- **AES-CBC (as defined in FIPS PUB 197, and NIST SP 800-38A) mode,**
- **AES-GCM (as defined in NIST SP 800-38D),**
- **AES-CCM (as defined in NIST SP 800-38C)**]

and cryptographic key sizes 128-bit key sizes **and [256-bit key sizes]**.

6.2.2.5 FCS_COP.1(2) Cryptographic operation (Hashing)

FCS_COP.1.1(2) Refinement: The **[TSF]** shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm [**SHA-256, SHA-384, SHA-512**] and **message digest** sizes [**256, 384, 512] bits** that meet the following: ***FIPS Pub 180-4***.

6.2.2.6 FCS_COP.1(3) Cryptographic operation (Digital Signature)

FCS_COP.1.1(3) Refinement The **[TSF]** shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm [

- **RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4;**
- **ECDSA schemes** using **"NIST curves" P-384 and [P-256, P-521]** that meet the following: **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5**

].

6.2.2.7 FCS_COP.1(4) Cryptographic operation (Keyed-Hash Message Authentication)

FCS_COP.1.1(4) Refinement: The **[TSF]** shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm **HMAC-[SHA-1, SHA-256, SHA-384]**, key sizes [*160, 256, 384*] **and message digest** sizes **[160, 256, 384] bits** that meet the following: **FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-4, "Secure Hash Standard."**

6.2.2.8 FCS_HTTPS_EXT.1 HTTPS protocol

FCS_HTTPS_EXT.1.1 The [MDM Server] shall implement the HTTPS protocol that complies with RFC 2818.

FCS_ HTTPS_EXT.1.2 The [MDM Server] shall implement HTTPS using TLS as specified in FCS_TLSS_EXT.1.

6.2.2.9 FCS_IV_EXT.1 Initialization vector generation

FCS_IV_EXT.1.1 The MDM Server shall generate IVs in accordance with Table 12.

Cipher Mode	Reference	IV Requirements
Electronic Codebook (ECB)	SP 800-38A	No IV
Counter (CTR)	SP 800-38A	"Initial Counter" shall be non-repeating. No counter value shall be repeated across multiple messages with the same secret key.
Cipher Block Chaining (CBC)	SP 800-38A	IVs shall be unpredictable. Repeating IVs leak information about whether the first one or more blocks are shared between two messages, so IVs should be non-repeating in such situations.
Output Feedback (OFB)	SP 800-38A	IVs shall be non-repeating and shall not be generated by invoking the cipher on another IV.
Cipher Feedback (CFB)	SP 800-38A	IVs should be non-repeating as repeating IVs leak information about the first plaintext block and about common shared prefixes in messages.
XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing (XTS)	SP 800-38E	No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer.
Cipher-based Message Authentication Code (CMAC)	SP 800-38B	No IV
Key Wrap and Key Wrap with Padding	SP 800-38F	No IV
Counter with CBC-Message Authentication Code	SP 800-38C	No IV. Nonces shall be non-repeating.

Cipher Mode	Reference	IV Requirements
(CCM)		
Galois Counter Mode (GCM)	SP 800-38D	IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key unless an implementation only uses 96-bit IVs (default length).

Table 12 – References and IV Requirements for NIST-approved Cipher Modes

6.2.2.10 FCS_RBG_EXT.1(1) Extended: Random Bit Generation

FCS_RBG_EXT.1.1(1) The TSF shall perform all deterministic random bit generation services in accordance with *NIST Special Publication 800-90A using* [*Hash_DRBG (SHA-1)*].

FCS_RBG_EXT.1.2(1) The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [a platform-based RBG] with a minimum of [256 bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

6.2.2.11 FCS_STG_EXT.1(1) Cryptographic key storage

FCS_STG_EXT.1.1(1) The [TSF] shall store persistent secrets and private keys when not in use, in [platform-provided key storage, as specified in FCS_STG_EXT.2].

6.2.2.12 FCS_STG_EXT.2 Encrypted Cryptographic key storage

FCS_STG_EXT.2.1 The MDM Server shall encrypt all keys using AES in the [*CBC mode*].

6.2.2.13 FCS_TLSC_EXT.1 Cryptographic Support

FCS_TLSC_EXT.1.1 The [TSF] shall implement [TLS 1.0 (RFC 3246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- [Optional Ciphersuites:
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

FCS_TLSC_EXT.1.2 The [TSF] shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The [TSF] shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.1.4 The [TSF] shall support mutual authentication using X.509v3 certificates.

FCS_TLSC_EXT.1.5 The [TSF] shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [secp256r1, secp384r1] and no other curves.

6.2.2.14 FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The [MDM Server] shall implement [*TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites: [

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- [Optional Ciphersuites:
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA as defined in RFC 5246*
  - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
  - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
  - *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
  - *TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*
  -
  - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

]].

FCS_TLSS_EXT.1.2 The [MDM Server] shall deny connections from clients requesting SSL 1.0, SSL 2.0, SSL 3.0 and [no other TLS version].

FCS_TLSS_EXT.1.3 The [MDM Server] shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.1.4 The [MDM Server] shall not establish a trusted channel if the peer certificated is invalid.

FCS_TLSS_EXT.1.5 The [MDM Server] shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the peer.

FCS_TLSS_EXT.1.6 The [MDM Server] shall generate key agreement parameters [*over NIST curves [secp384r1] and no other curves; Diffie- Hellman parameters of size 2048 bits and [no other size]*].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_ENR_EXT.1 Enrollment of Mobile Device into Management

FIA_ENR_EXT.1.1 The MDM Server shall authenticate the remote user over a trusted channel during the enrollment of a mobile device.

FIA_ENR_EXT.1.2 The MDM Server shall limit the user's enrollment of devices to [specific device models, a number of devices, specific time period].

6.2.3.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 Refinement: The [TSF] shall allow [*no* **TSF** *mediated action*] on behalf of the user to be performed before the user is authenticated **with the Server**.

FIA_UAU.1.2 Refinement: The [TSF] shall require each user to be successfully authenticated **with the Server** before allowing any other **TSF** - mediated actions on behalf of that user.

6.2.3.3 FIA_X509_EXT.1 X509 Validation

FIA_X509_EXT.1.1 The [*TSF*] shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id- kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

o Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

FIA_X509_EXT.1.2(1) The [*TSF*] shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.2.3.4 FIA_X509_EXT.2 X509 Authentication

FIA_X509_EXT.2.1 The [*TSF*] shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*TLS, HTTPS*], and [*code signing for system software updates, policy signing*].

FIA_X509_EXT.2.2 When the [*TSF*] cannot establish a connection to determine the validity of a certificate, the [*TSF*] shall [*not accept the certificate*].

FIA_X509_EXT.2.3 *The [TSF] shall require a unique certificate for each client device.*

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1(1) Management of security functions behaviour (Management of Functions in MDM Server)

FMT_MOF.1.1(1) **Refinement:** The **MDM Server** shall restrict the ability to perform the functions

- listed in FMT_SMF.1(1)
- enable, disable, and modify policies listed in FMT_SMF.1(1)
- listed in FMT_SMF.1(2*)*

to *Authorised Administrators*.

6.2.4.2 FMT_MOF.1(2) Management of security functions behaviour (Management of Enrollment function)

FMT_MOF.1.1(2) **Refinement:** The **MDM Server** shall restrict the ability to initiate the enrollment process to *Authorized Administrators and MD users*.

6.2.4.3 FMT_POL_EXT.1 Trusted policy update

FMT_POL_EXT.1.1 The MDM Server shall provide digitally signed policies and policy updates to the MDM Agent.

6.2.4.4 FMT_SMF.1(1) Specification of Management Functions (Server configuration of Agent)

FMT_SMF.1.1(1) **Refinement:** The **MDM Server** shall be capable of **communicating the** following **commands to the MDM Agent**:

1. transition to the locked state, (*MDF Function 8*)
2. full wipe of protected data, (*MDF Function 9*)
3. unenroll from management,
4. install policies,
5. query connectivity status,
6. query the current version of the MD firmware/software,
7. query the current version of the hardware model of the device,
8. query the current version of installed mobile applications,

9. import X.509v3 certificates into the Trust Anchor Database, (*MDF Function 13*)
10. install applications, (*MDF Function 18*)
11. update system software, (*MDF Function 17*)
12. remove applications, (*MDF Function 16*)
13. remove Enterprise application, (*MDF Function 19*)

and the following commands to the MDM Agent: [

14. wipe Enterprise data, (*MDF Function 28*)
15. remove imported X.509v3 certificates and [[all other X.509v3 certificates]] in the Trust Anchor Database, (*MDF Function 14*)
16. alert the administrator,
17. import keys/secrets into the secure key storage, (*MDF Function 11*)
18. destroy imported keys/secrets and [no other keys/secrets] in the secure key storage, (*MDF Function 12*)
22. place applications into application process groups based on [application name and version], (*MDF Function 43*)

and the following MD configuration policies:

24. password policy:
    a. minimum password length
    b. minimum password complexity
    c. maximum password lifetime (*MDF Function 1*)
25. session locking policy:
    a. screen-lock enabled/disabled
    b. screen lock timeout
    c. number of authentication failures (*MDF Function 2*)
26. wireless networks (SSIDs) to which the MD may connect (*MDF Function 6*)
27. security policy for each wireless network:
    a. [specify the CA(s) from which the MD will accept WLAN authentication server certificate(s]
    b. ability to specify security type
    c. ability to specify authentication protocol
    d. specify the client credentials to be used for authentication
    e. [no additional WLAN management functions] (*MDF Function 7*)
28. application installation policy by [
    a. specifying authorized application repository(s)
    ], (*MDF Function 10*)
29. enable/disable policy for [camera, microphone] across MD, [no other method], (*MDF Function 5*)

and the following MD configuration policies: [

30. enable/disable policy for the VPN protection across MD, [no other method], (*MDF Function 3*)
31. enable/disable policy for [mobile networks, Wi-Fi, GPS, FM radio, NFC and Bluetooth], (*MDF Function 4*)
32. enable/disable policy for data signaling over [USB, SD Card, HDMI], (*MDF Function 22*)
33. enable/disable policy for [Media sharing, Miracase, BlackBerry Bridge, Wi-Fi hotspot, Bluetooth], (*MDF Function 23*)
34. enable/disable policy for developer modes, (*MDF Function 24*)
35. enable policy for data-at rest protection, (*MDF Function 25*)

36. enable policy for removable media's data-at-rest protection, (*MDF Function 26*)
37. enable/disable policy for local authentication bypass, (*MDF Function 27*)
38. the Bluetooth trusted channel policy:
    a. enable/disable the Discoverable mode (for BR/EDR)
    [i. no other Bluetooth configuration] (*MDF Function 20*)
39. enable/disable policy for display notification in the locked state of
    [
    a. email notifications,
    b. calendar appointments,
    c. contact associated with phone call notification,
    d. text message notification
    e. other application-based notifications
    ] (*MDF Function 21*)
40. policy for establishing a trusted channel or disallowing establishment if the MD cannot establish a connection to determine the validity of a certificate, (*MDF Function 30*)
43. [certificate] used to validate digital signature on applications, (*MDF Function 33*)
46. the unlock banner policy, (*MDF Function 36*)
47. configure the auditable items (*MDF Function 37*)
48. enable/disable [
    a. USB mass storage mode,
    ] (*MDF Function 39*)
49. enable/disable backup to [locally connected system, remote system] (*MDF Function 40*)
51. enable/disable location services:
    a. across device
    [
    c. no other method] (*MDF Function 44*)
52. enable/disable policy for user unenrollment
53. [
    (a) enable/disable automatic transfer of diagnostic data to an external device or service other than an MDM service with which the device has enrolled;
    (d) full wipe of all user data and applications (applications not included in the out-of-the-box install).
    ].

6.2.4.5 FMT_SMF.1(2) Specification of Management Functions (Server configuration of server)

FMT_SMF.1.1(2) Refinement: The **MDM Server** shall be capable of **performing** the following management functions: [

a. configure X.509v3 certificates for MDM Server use
b. configure the [specific devices, a number of devices, specific time period] allowed for enrollment

[

d. configure the TOE unlock banner,

e. configure periodicity of the following commands to the agent: [
    5. query connectivity status;
    6. query the current version of the MD firmware/software;

7. query the current version of the hardware model of the device;
8. query the current version of installed mobile applications],

g. no other management functions].

6.2.4.6 FMT_SMR.1 Security roles

FMT_SMR.1.1 Refinement: The **MDM Server** shall maintain the roles *administrator, MD user, and [Server primary administrator, Security configuration administrator, Device user group administrator, Auditor]*].

FMT_SMR.1.2 Refinement: The **MDM Server** shall be able to associate users with roles.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_TST_EXT.1 TSF testing

FPT_TST_EXT.1.1 The [MDM Server] shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The [MDM Server] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the [TSF]-provided cryptographic services.

6.2.5.2 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The MDM Server shall provide Authorized Administrators the ability to query the current version of the MDM Server software.

FPT_TUD_EXT.1.2 The [MDM Server] shall provide Authorized Administrators the ability to initiate updates to TSF software.

FPT_TUD_EXT.1.3 The [MDM Server] shall provide a means to verify software updates to the TSF using a digital signature mechanism prior to installing those updates.

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the [MDM Server] shall display an Administrator-specified advisory notice and consent warning message regarding use of the TOE.

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_ITC.1(1) Inter-TSF Trusted channel (Authorized IT Entities)

FTP_ITC.1.1(1) Refinement: The **[MDM Server]** shall **use [TLS] to** provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [authentication server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data **from disclosure and detection of modification of the channel data**.

FTP_ITC.1.2(1) The TSF shall permit **the MDM Server or other authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel **for [the transfer of audit information].**

6.2.7.2 FTP_ITC.1(2) Inter-TSF Trusted channel (Authorized IT Entities)

FTP_ITC.1.1(2) The TSF shall **use [*TLS*] to** provide a **trusted** communication channel between itself and another trusted IT product that is logically distinct from other communication channels**,** provides assured identification of its end points**,** protects channel data from disclosure, and detects modification of the channel data.

FTP_ITC.1.2(2) The TSF shall permit **the TSF and MDM Agent** to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for **all communication between the MDM Server and the MDM Agent and [no other communication]].**

6.2.7.3 FTP_TRP.1(1) Trusted Path for Remote Administration

FTP_TRP.1.1(1) Refinement: The **[MDM Server]** shall **use [TLS/HTTPS] to** provide a communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.

FTP_TRP.1.2(1) Refinement: The **[MDM Server]** shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3(1) Refinement: The **[MDM Server]** shall require the use of the trusted path for all remote administration actions.

6.2.7.4 FTP_TRP.1(2) Trusted Path for Enrollment

FTP_TRP.1.1(2) Refinement: The **[MDM Server]** shall **use [TLS/HTTPS] to** provide a communication path between itself and **MD users** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.

FTP_TRP.1.2(2) Refinement: The **[MDM Server]** shall permit **MD users** to initiate communication via the trusted path.

FTP_TRP.1.3(2) Refinement: The **[MDM Server]** shall require the use of the trusted path for all MD user actions.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following table provides a mapping between the SFRs and Security Objectives. Additional mappings are provided to complete those provided in the Protection Profile for Mobile Device Management.

	O.APPLY_POLICY	O.ACCOUNTABILITY	O.DATA_PROTECTION_TRANSIT	O.INTEGRITY	O.MANAGEMENT
FAU_ALT_EXT.1		X			
FAU_GEN.1(1)		X			
FAU_NET_EXT.1		X			
FAU_SAR.1		X			
FAU_STG_EXT.1		X	X		
FAU_STG_EXT.2		X			
FCS_CKM.1			X		
FCS_CKM.2			X		
FCS_CKM_EXT.4			X		
FCS_COP.1(1)			X		
FCS_COP.1(2)			X		
FCS_COP.1(3)			X		
FCS_COP.1(4)			X		
FCS_HTTPS_EXT.1			X		
FCS_IV_EXT.1			X		
FCS_RBG_EXT.1			X		
FCS_STG_EXT.1			X		
FCS_STG_EXT.2			X		
FCS_TLSC_EXT.1			X		
FCS_TLSS_EXT.1			X		
FIA_ENR_EXT.1	X				
FIA_UAU.1					X
FIA_X509_EXT.1			X		
FIA_X509_EXT.2			X	X	
FMT_MOF.1(1)					X
FMT_MOF.1(2)	X				X
FMT_POL_EXT.1	X				
FMT_SMF.1(1)	X				X
FMT_SMF.1(2)					X
FMT_SMR.1					X
FPT_TST_EXT.1				X	
FPT_TUD_EXT.1				X	
FTA_TAB.1					X
FTP_ITC.1(1)			X		
FTP_ITC.1(2)			X		
FTP_TRP.1(1)			X		

	O.APPLY_POLICY	O.ACCOUNTABILITY	O.DATA_PROTECTION_TRANSIT	O.INTEGRITY	O.MANAGEMENT
FTP_TRP.1(2)			X		

Table 13 – Mapping of SFRs to Security Objectives

6.4 DEPENDENCY RATIONALE

Table 14 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_ALT_EXT.1	None	N/A	
FAU_GEN.1(1)	FAU_GEN.1	✓	
FAU_NET_EXT.1	None	N/A	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG_EXT.1	FAU_GEN.1	✓	
FAU_STG_EXT.2	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FCS_CKM_EXT.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FCS_COP.1(3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FCS_COP.1(4)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FCS_HTTPS_EXT.1	None	N/A	
FCS_IV_EXT.1	None	N/A	
FCS_RBG_EXT.1	None	N/A	
FCS_STG_EXT.1	None	N/A	
FCS_STG_EXT.2	FCS_IV_EXT.1	✓	
FCS_TLSC_EXT.1	None	N/A	
FCS_TLSS_EXT.1	None	N/A	
FIA_ENR_EXT.1	None	N/A	
FIA_UAU.1	FIA_UID.1	No	The Protection Profile for Mobile Device Management assumes that users must be identified to be authenticated, and exact conformance to this PP does not permit inclusion of FIA_UID.1.
FIA_X509_EXT.1	None	N/A	
FIA_X509_EXT.2	FIA_X509_EXT.1	✓	
FMT_MOF.1(1)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_MOF.1(2)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_POL_EXT.1	None	N/A	
FMT_SMF.1(1)	None	N/A	
FMT_SMF.1(2)	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	The Protection Profile for Mobile Device Management assumes that users must be identified to be authenticated, and exact conformance to this PP does not permit inclusion of FIA_UID.1. This dependency is met by FIA_UAU.1.
FPT_TST_EXT.1	None	N/A	
FPT_TUD_EXT.1	None	N/A	
FTA_TAB.1	None	N/A	
FTP_ITC.1(1)	None	N/A	
FTP_ITC.1(2)	None	N/A	
FTP_TRP.1(1)	None	N/A	
FTP_TRP.1(2)	None	N/A	

Table 14 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the Security Assurance Requirement specified in the Protection Profile for Mobile Device Management.

The assurance requirements are summarized in Table 15.

Assurance Class	Assurance Components	
	Identifier	Name
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition

Assurance Class	Assurance Components	
	Identifier	**Name**
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - sample
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

Table 15 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

A description of each of the TOE security functions follows.

7.1 SECURITY AUDIT

7.1.1 Server Alerts

When the MDM Server receives notice of a change in enrollment status, or the failure to apply policies to a mobile device, an entry is made in the server logs.

Configuration of event notification is performed by an administrator using SQL commands as specified in the guidance documentation. The administrator selects the events that will be alerted and the email address to which the alerts will be sent. When one of these events occurs, an email is automatically sent to the configured administrator email address.

TOE Security Functional Requirements addressed: FAU_ALT_EXT.1.

7.1.2 Audit Data Generation and Audit review

The BES generates audit records for all device management events. These records are stored in the BES database. The BES logs all actions performed by an administrator, all of the commands issued from the BES to the mobile devices, and all of the cryptographic operations described in the Protection Profile for Mobile Device Management.

In addition to the records held in the BES_DB, there are Installer Logs that include records related to the installation of the BES.

7.1.2.1 BES_DB

The BES_DB is the BES database. All logging entries are stored in the database tables of the database. The logs can be read using the web interface, or they can be exported to the Administrator's location over the TLS connection used to secure remote administration. The logs are exported in a .CSV file. The export function is initiated from the Audit screen of the administrative interface.

The BES_DB, when exported, appears in a spreadsheet in the following format:

Record ID	Date created	Category	Event	Correlation ID	Host	User	Tenant	Success	Details
179	2016-10-25 18:56:33:793 UTC	System Access	User logged in	590f436d-6fa6-4dbe-980a-c442f83b93bf	BC-ITHOMSON03.devlab2k.testnet.rim.net	admin	BCOP1190	TRUE	Trusted Channel Protocol=TLS;Identify of Administrator=admin

Figure 18 – Sample BES_DB Output

Table 16 provides a description of the fields.

Field	Description	Example

Field	Description	Example
Record ID	Unique entry identifier	179
Date created	The timestamp indicating when the event was generated	2016-10-25 18:56:33:793 UTC
Category	Method of grouping similar types of events. Can be used for searching or classification	System Access
Event	Description of event being logged	User logged in
Correlation ID	A workflow correlation Id that can be used to track a set of events when examining a workflow	590f436d-6fa6-4dbe-980a-c442f83b93bf
Host	Name of host on which the event was initiated	BC-ITHOMSON03.devlab2k.testnet.rim.net
User	User that performed activity being logged	admin
Tenant	The id of the tenant for whom the event was generated. Null if not applicable.	BCOP1190
Success	Indicator of whether or not action was successful	TRUE
Details	Description of the event logged	Trusted Channel Protocol=TLS;Identify of Administrator=admin

Table 16 – BES_DB Record Format

7.1.2.2 Log Mapping

Logs addressing each of the SFRs may be found in the BES_DB.

Requirement	Description
FAU_ALT_EXT.1	Type of alert
FAU_GEN.1(1)	Start-up and shutdown of the MDM Server software
FAU_GEN.1(1)	All administrative actions
FAU_GEN.1(1)	Commands issued from the MDM Server to an MDM Agent
FCS_CKM.1(1)	Failure of the key generation activity for

Requirement	Description
	authentication keys
FCS_HTTPS_EXT.1	Failure of the certificate validity check
FCS_RBG_EXT.1(1)	Failure of the randomization process
FCS_TLSC_EXT.1	Failure to establish a TLS session. Failure to verify presented identifier.
FCS_TLSS_EXT.1(1)	Failure to establish a TLS session
FIA_ENR_EXT.1.1	Failure of MD user authentication.
FIA_X509_EXT.1(1)	Failure of X.509 certificate validation
FIA_X509_EXT.2(1)	Failure to establish connection to determine revocation status.
FMT_MOF.1(1)	Issuance of command to perform function. Change of policy settings
FMT_MOF.1(2)	Enrollment by a user
FMT_SMF.1(2)	Success or failure of function
FPT_TST_EXT.1	Execution of this set of TSF self-tests. Failure of self-test. Detected integrity violation.
FPT_TUD_EXT.1	Initiation of update Success or failure of update
FTP_ITC.1(1)	Initiation and termination of the trusted channel
FTP_ITC.1(2)	Initiation and termination of the trusted channel
FTP_TRP.1(1)	Initiation and termination of the trusted channel.
FTP_TRP.1(2)	Initiation and termination of the trusted channel

Table 17 – Log Mapping

In the evaluated configuration, the BES is configured to send new audit records from the BES server to a syslog server every 15 minutes. This is done over a TLS encrypted link.

TOE Security Functional Requirements addressed: FAU_GEN.1(1), FAU_SAR.1, FAU_STG_EXT.1.

7.1.3 Network Reachability Review

The MDM Agent on the mobile device contacts the MDM Server:

- Whenever there is a network coverage change
- At a polling cycle interval of every one minute, 15 minutes or eight hours, depending upon the connection conditions

When a device successfully communicates with the MDM Server, the 'Last Contact Time' statistic is update for the device record. This information can be seen in the BES12 Administrative console by adding the 'Last Contact' field to the main Users and device table.

TOE Security Functional Requirements addressed: FAU_NET_EXT.1.

7.1.4 Audit Trail Storage

In the evaluated configuration, the BES is configured to send new audit records from the BES server to a syslog server every 15 minutes. This is done over a TLS encrypted link. The trusted channel is described in Section 7.2.8.2.

TOE Security Functional Requirements addressed: FAU_STG_EXT.1.

Audit records are stored in the BES12 database and protected by the operating system. Protection from unauthorized modification or deletion of the audit entries stored in the database is controlled by ensuring that only the authorized database administrator has access to the BES12 data. Additionally, the ability to purge audit logs stored in the database is controlled by the 'Edit audit settings and purge data' permission available to users in select BES12 security roles.

TOE Security Functional Requirements addressed: FAU_STG_EXT.2.

7.2 CRYPTOGRAPHIC SUPPORT

Cryptographic support is provided by a cryptographic module within the BES12. The module is the Security Builder GSE-J Crypto Core, version 2.9.1, and it uses cryptographic algorithms which have been validated to the associated CAVP standards. The Cryptographic Algorithm Validation Program (CAVP) certificate details are as follows:

Usage	CAVP Certificate
AES	5342
DRBG	2062
DSA	1378
ECDSA	1403
HMAC	3539
KAS	174
RSA	2858
SHA	4293

Table 18 – CAVP Certificate Numbers

The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.

7.2.1 Cryptographic key generation and establishment

RSA, ECC and FFC asymmetric keys are used with the following key lengths:

Key Type	Usage	Strength
ECC	Root certificate	secp521r1
ECC	Intermediate certificate	secp521r1
ECC	Server certificate	secp521r1
ECDHE	TLS	Between 128 and 256 bit (effective strength)
FFC	TLS	2048
RSA	Root certificate	4096
RSA	Intermediate certificate	3072
RSA	Server certificate	2048

Table 19 – Key Usage and Sizes

For RSA-based key establishment schemes, the TOE acts as a sender for FCS_TLSS_EXT.1 and as a recipient for FCS_TLSC_EXT.1. RSA key establishment is implemented in accordance with NIST Special Publication 800-56B. To mitigate the risk of RSA timing attacks, the TOE does not reveal the particular error that has occurred, either through the contents of error messages or through timing variations.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.2.

7.2.2 Cryptographic key destruction

7.2.2.1 Cryptographic Key Destruction

Table 20 lists each key required to implement the claimed functionality, when the key is zeroized and the method used to zeroize the key.

Key or Secret	Timing of Zeroization	Zeroization Procedure
Database encryption password	Stored in memory while Server is running. It is zeroized on process termination.	When the database encryption password is being used it is stored in volatile memory and is not zerioized. It is cleared on shutdown of the BES core service.
	The database encryption password is stored on the file system encrypted using Elliptic Curve cryptography (ECC).	The database encryption password is stored encrypted on the file system and is not zeroized.

Key or Secret	Timing of Zeroization	Zeroization Procedure
Encryption key for Database encryption password	The ECC key used to encrypt the database encryption password is stored in the platform-provided keystore. (ECC was chosen for this function because the Windows platform provided key storage only supports storage of asymmetric keys.)	The ECC key is zeroized by the TSF after each use. It is zeroized by being overwritten by zeroes.
Database keystore password	Stored in memory while Server is running. It is zeroized on process termination.	The database keystore password is not zerioized and is cleared on shutdown of the BES core service.
	Stored encrypted in the database.	Is stored encrypted and is removed when the database is deleted during uninstallation of BES.
Asymmetric cryptography private keys	Keys are stored encrypted in the database	Is stored encrypted and is removed when the database is deleted during uninstallation of BES.
	Keys in memory are zeroized on process termination	Value in memory replaced by zeros
decrptEnginePrivateCert	Keys are stored encrypted in the database	Not applicable
	Keys in memory are zeroed out immediately after used	Value in memory replaced by zeros
TLS Symmetric session key	On session invalidation	Value in memory replaced by zeros
TLS key negotiation key (RSA, ECDH, FFC)	On completion of negotiation	Value in memory replaced by zeros

Table 20 – Key Destruction

TOE Security Functional Requirements addressed: FCS_CKM_EXT.4.

7.2.3 Cryptographic operation

7.2.3.1 Cryptographic operation (Confidentiality Algorithms)

The following table shows the symmetric encryption algorithms that the BlackBerry Cryptographic Kernel implements.

Algorithm	Key Length (in bits)	Modes
AES	128, 256	CBC
AES	128, 256	GCM
AES	128, 256	CCM

Table 21 – Confidentiality Algorithms

TOE Security Functional Requirements addressed: FCS_COP.1(1).

7.2.3.2 Cryptographic operation (Hashing)

The MDM Server supports SHA-256, SHA-384 and SHA-512 hashing algorithms. All are operated in byte-oriented mode. They are associated with other functions, such as keyed hash message authentication and the use of digital signatures through the use of the ciphersuites supported by the implementation of TLS. SHA-256 and SHA-384 are used in TLS to perform TLS packet integrity checks. SHA-512 is used in X.509 certificate validation.

TOE Security Functional Requirements addressed: FCS_COP.1(2).

7.2.3.3 Cryptographic Operation (Digital Signature)

The following table shows the signature algorithms that the BlackBerry Cryptographic Kernel implements.

Signature Algorithm	Supported curve or key length (in bits)
RSA algorithms	PKCS1.5 using 2048, 3072 and 4096. PSS using 2048, 3072, and 4096. With hash algorithms: SHA-256, SHA-384, and SHA-512
ECDSA	FIPS 186-4 using P-256, P-384, P-521 with hash algorithms: SHA-256, SHA-384, and SHA-512.

Table 22 – Supported Curves and Key Lengths

TOE Security Functional Requirements addressed: FCS_COP.1(3).

7.2.3.4 Cryptographic Operation (Keyed-Hash Message Authentication)

The following table shows the keyed-hash message authentication algorithms that the BlackBerry Cryptographic Kernel implements.

Algorithm	Key Length	Hash Function	Block Size (bits)	Output MAC Length
HMAC-SHA-1	160	SHA-1	512	160

Algorithm	Key Length	Hash Function	Block Size (bits)	Output MAC Length
HMAC-SHA-256	256	SHA-256	512	256
HMAC-SHA-384	384	SHA-384	1024	384

Table 23 – Keyed-Hash Message Authentication

TOE Security Functional Requirements addressed: FCS_COP.1(4).

7.2.4 HTTPS

HTTPS is implemented in support of the connection between the BES and the Administrator Workstation.

TOE Security Functional Requirements addressed: FCS_HTTPS_EXT.1.

7.2.5 Initialization Vector Generation

The TSF generates initialization vectors for TLS which conform to SP 800-38D for AES-GCM. The DRBG is used when generating the IVs.

Table 24 details the encryption of user credentials, persistent secrets, and private keys and the generation of the IVs used for that encryption.

Key or Secret	Usage	Generation of IVs
Database encryption password	Encrypts all sensitive information stored in the database	IVs are generated randomly.
Database keystore password	Encrypts all private keys stored database keystore	IVs are generated randomly.
Asymmetric cryptography private keys	Used for SSL/TLS	IVs are generated randomly.
decrptEnginePrivateCert	It is used to decrypt private information for the device	IVs are generated randomly.
GME deviceEncryptionKey	It is used by the device to encrypt private information sent to the device	IVs are generated randomly.
Administrative credentials	Used to access the BES administrative functions	IVs are generated randomly.

Table 24 – Initialization Vectors

TOE Security Functional Requirements addressed: FCS_IV_EXT.1.

7.2.6 Random bit generation

7.2.6.1 Random bit generation

Random bit generation is provided by the BlackBerry Cryptographic Java Module, and is referenced by DRBG CAVP certificate number 2062.

The platform-based RBG provides entropy to the TOE RBG, and is provided by the Windows Server 2012 R2 platform. This platform-based RBG is described in the Security Policy for the CNG.SYS component, CMVP certificate number 2605.

TOE Security Functional Requirements addressed: FCS_RBG_EXT.1.

7.2.7 Cryptographic key storage

7.2.7.1 Cryptographic key storage

Table 25 lists each key required to implement the claimed functionality, how the key is used and where the key is stored. Persisted secrets are encrypted using AES-CBC. Asymmetric private keys are encrypted using Password based cryptography with HMAC-SHA-256 and AES-256 (CBC).

Key or Secret	Usage	Storage
ECC key used to encrypt the database encryption password	Encrypts the database encryption password	Stored encrypted in the platform-provided keystore, plaintext in memory.
Database encryption password	Encrypts all sensitive information stored in the database	Encrypted using ECC when stored on the file system, and plaintext in memory
Database keystore password	Encrypts all private keys stored database keystore	Stored encrypted in the database, plaintext when in memory
Asymmetric cryptography private keys	Used for SSL/TLS	Stored encrypted in the database and plaintext in memory
decrptEnginePrivateCert	It is used to decrypt private information for the device	Stored encrypted in the database and plaintext in memory
GME deviceEncryptionKey	It is used by the device to encrypt private information sent to the device	Stored in the database and plaintext in memory Device GME keys are encrypted and stored in the database using the database encryption password. GME keys are fetched from the database, decrypted, used, then immediately zeroized.

Key or Secret	Usage	Storage
device password	Device lock password	The password hash (SHA-512) is stored in the database, plaintext in memory
Administrative credentials	Used to access the BES administrative functions	The password hash (SHA-512) is stored in the database, plaintext in memory

Table 25 – Key Storage

TOE Security Functional Requirements addressed: FCS_STG_EXT.1, FCS_STG_EXT.2.

7.2.8 TLS

7.2.8.1 TLS Client Protocol

The TLS client implementation within the TOE platform supports TLS 1.0, TLS 1.1 and TLS 1.2, and the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

The TOE acts as a TLS client when communicating with the authentication server.

The TOE automatically compares the Distinguished Name (DN) in the server certificate to the DN expected for the LDAP server. The TOE supports identifier verification as per RFC 6125 using DNS Name, Common Name or IP address. Wildcards are not supported in reference identifiers. Certificate pinning is not supported. The extension for signature algorithms (signature_algorithms) is enabled by default. Support for Elliptic Curves Extension is included by default.

The TOE supports the use of client side certificates for mutual authentication. Only LDAP servers that also support this function may be used in the evaluated configuration. Older versions of SSL are denied as part of the TLS handshake.

To configure the audit server, the DN of the audit server must be provided using the SQL commands specified in the user guidance.

TOE Security Functional Requirements addressed: FCS_TLSC_EXT.1(1).

7.2.8.2 TLS Server Protocol

The BES acts as a server in support of remote administration, device enrollment and device management.

For remote management, BES supports TLS 1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256

Mutual authentication is not supported for remote management.

The BES acts as a server in support of device enrollment and device management. For communications with devices, BES supports TLS 1.0, 1.1 and 1.2, and the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

The supported ECDHE curve is P-384, and the supported DH key size is DH mod 2048.

For authentication between the BES and the mobile device, the BES automatically compares the Distinguished Name (DN) in the certificate to the DN expected for the agent.

The server key exchange message is sent after the server certificate message to convey information required to complete the key exchange. The BES and the mobile devices both default to use TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384; therefore no parameter configuration is required.

Older versions of SSL and TLS are denied as part of the TLS handshake.

TOE Security Functional Requirements addressed: FCS_TLSS_EXT.1.

7.3 IDENTIFICATION AND AUTHENTICATION

7.3.1 Enrolment of mobile device into management

Devices may be enrolled into management using the BlackBerry using Wi-Fi Direct Enrollment.

7.3.1.1 Enrollment using Wi-Fi Direct

The administrator assigns the device to a user account and selects ‘Activate devices’ to activate the device. The administrator also selects a password for the device.

The device and associated password are then provided to the user, after verification of the user’s identity. When the user enters the provided password and logs in for the first time, any configured profiles and IT policies are downloaded to the device.

The user then performs the following steps to perform direct enrollment.

- Navigate to **Accounts > Advanced > Work**.
- Enter the username and password supplied by the administrator as well as the URL formatted as follows:

  http://<FQDNofBES>:8882/<SRP>/mdm

  where 'FQDNofBES' is the fully qualified domain name of the BES server and 'SRP' is the Server Routing Protocol Identifier of the BES server that is being used to provide management functionality.

Following initial communications and certificate signing, TLS is used to secure enrollment data that is passed between the device and the BES. When the activation profile is created by an administrator, the administrator may

- assign the number of devices that a user can activate
- assign device types that a user can activate

When a user's device is enrolled, an activation password is generated, and must be entered by the user in order to complete the activation. This password may be assigned an Activation period expiration, limiting the time period in which it may be used.

TOE Security Functional Requirements addressed: FIA_ENR_EXT.1

7.3.2 Timing of authentication

No actions can be performed before authentication.

TOE Security Functional Requirements addressed: FIA_UAU.1.

7.3.3 X.509 Certificates

7.3.3.1 X.509 Validation

When a server certificate is loaded onto the BES, the BES performs checks on the certificate. For CA certificates, the BES verifies that the basicConstraints extension is present and the CA flag is set to TRUE.

When a client certificate is presented to the TOE Platform, the TOE Platform performs checks on the certificate. This is done as part of the SSL handshake. These checks include verification that the extendedKeyUsage field of the certificate indicates server authentication, client authentication or software signing as appropriate, and that the key agreement bit is set. Client certificates presented for TLS have the Client Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

When a certificate is used for trusted update, BES verifies that the extendedKeyUsage field of the client certificate includes "Code Signing".

For CA certificates, the BES verifies that the basicConstraints extension is present and the CA flag is set to TRUE.

The BES verifies the validity of the certificate presented by the BB 10 device as part of the TLS protocol, after the client hello is accepted. The certificate path validation algorithm used by the BES is the path validation algorithm described in RFC 5820.

BES stores certificates in its database. The database entry specifies the use of the certificate. For example, the audit TLS client certificate is used to authenticate to the audit server.

TOE Security Functional Requirements addressed: FIA_X509_EXT.1(1), FIA_X509_EXT.1(2).

7.3.3.2 X.509 Authentication

When certificates are loaded into the BES, they are loaded for a particular purpose. This is used to determine which certificates are used by the BES. Each TLS port hard codes a specific certificate which it uses to establish a trusted channel for TLS communication. When the BES cannot establish a link to the Online Certificate Status Protocol server to determine a certificate's validity, the certificate is rejected.

TOE Security Functional Requirements addressed: FIA_X509_EXT.2.

7.4 SECURITY MANAGEMENT

The Security management functionality applies to all of the claimed mobile devices.

7.4.1 Management of Functions in MDM Server

Only administrators and users whose accounts have been configured for device activation by the administrator are able to enrol a device. An activation profile must be created and assigned to the user to allow the user to enrol a device. As part of the enrolment process, the user is authenticated by the Enterprise authentication system.

Security management functionality is restricted to authorized administrators, and only those actions described in the user guidance are available to those authorized administrators.

TOE Security Functional Requirements addressed: FMT_MOF.1(1)

7.4.2 Management of enrolment function

In order to be enrolled in the MDM services, the user must first be added either as a local user account, or using the organization's directory. This creates an activation username and password which must be sent securely to the user. Only these users whose accounts have been configured for device activation by the administrator are able to enrol a device. As part of the enrolment process, the user is authenticated by the Enterprise authentication system. This prevents unauthorized users from enrolling in the MDM services.

TOE Security Functional Requirements addressed: FMT_MOF.1(2)

7.4.3 Trusted policy update

After a user activates a device, the BlackBerry Device Service automatically sends to the device the IT policy that was assigned to the user account or group. If an IT policy was not assigned to the user account or group, the BlackBerry Device Service sends the Default IT policy.

When the settings for an IT policy rule are updated, the updated IT policy is sent to every device for each assigned user. The work space locks when it receives an IT policy that includes updated password rules. The BES uses its private key to sign the policy payloads using SHA512 with ECDSA algorithm. The device is able to verify the signature using the corresponding public key certificate.

If a policy update fails, an alert is sent to the BES administrator. If a failed policy update compromises the integrity of the device, this is detected by the BB 10 OS integrity checks and an alert is sent to the BES 12. The response to such an alert is administrator configurable, and options include quarantining the device from access to work resources, wiping work data or wiping the entire device.

TOE Security Functional Requirements addressed: FMT_POL_EXT.1

7.4.4 Specification of management functions (Server configuration of Agent)

There is no difference between the management functions and policies for the various BlackBerry 10 devices listed in Section 1.

The BES12 is capable of performing the following functions:

- Transition to the locked state – in the Administrative GUI, under ‘Users and Devices’, there is an option to lock a device. (1)
- Full wipe of protected data – this function may be initiated using ‘Delete all device data’ or ‘Delete only work data’. (2)
- Unenroll from management – this function is performed using the ‘Delete only work data’ command, which deleted the connection between the device and the user account in BES12. (3)
- Install policies – policies are set through the ‘Policies and Profiles’ pages of the Administrative GUI. (4)
- Query status – under ‘Users and Devices’, ‘Manage device’, there is an option to update device information. This is used to both send policy and profile information to the device and receive status information from the device, including connectivity status, OS version, hardware model, and installed applications. (5, 6, 7, 8)
- Import X.509v3 certificates into the Trust Anchor Database – certificates may be sent to devices and stored in the equivalent of a Trust Anchor Database during activation, using SCEP profiles or using User credential profiles. This functionality may be used to update certificates. (9)
- Install applications – installation of applications may be initiated by adding them to the ‘app list’ associated with the user account, user group or device group. (10)
- Update system software – Administrators may initiate a system software update. (11)
- Remove applications – Removal of applications may be initiated by removing them from the ‘app list’ associated with the user account, user group or device group. (12)

- Remove Enterprise applications – Only Administrators may remove Enterprise applications. (13)
- Wipe Enterprise data – The Administrator may initiate a wipe of Enterprise data. (14)
- Remove administrator-imported X.509v3 certificates in the Trust Anchor Database – a command to remove certificates stored in the equivalent of a Trust Anchor Database may be sent to devices using SCEP profiles or using User credential profiles. (15)
- Alert the administrator – if a mobile device detects a problem with the integrity of a device, it alerts BES12. The BES12 may be configured to issue a command to 'Delete all device data' or 'Delete only work data' on receipt of the alert. (16)
- Import keys/secrets into secure storage – Keys may be imported by Administrators of the management platform through policy configuration. (17)
- Destroy imported keys/secrets – Only an Administrator may destroy key imported by an Administrator. (18)
- Place applications into application process groups – Administrators may place applications into 'app lists' associated with user or device groups. (22)
- Password policy – an IT policy rule may include restrictions on the password used to protect corporate data. The rule may enforce a minimum password length, minimum password complexity and maximum password lifetime. (24)
- Session locking policy – a security timeout may be set within an IT policy rule. This policy determines the period of BlackBerry device user inactivity that must elapse before the work space locks. If the 'Allow app security timer reset' rule is selected, the device does not lock when apps that can reset the security timer are running. If the 'Maximum password attempts' may be set to specify the number of times that a BlackBerry device user can enter an incorrect password before a device deletes the data in the work space. (25)
- Wireless networks to which the MD may connect – an IT policy rule may be created to allow or block access to specified wireless networks identified by their SSIDs. (26)
- Security policy for each wireless network – an IT policy rule may be set to specify the CA(s) from which the mobile device will accept WLAN authentication server certificates, specify the required security type, specify the required authentication protocol, specify the client credentials to be used for authentication and limit the connection to a specific protocol settings profile such as WPA2-Enterprise. (27)
- Application installation policy – an IT policy rule may be set to allow applications to be downloaded from only specified application repositories. (28)

- Enable/disable policy for camera, microphone – an IT policy rule may be set to allow or prevent the use of the camera or microphone. (29)
- Enable/disable policy for the VPN protection – an IT policy rule may be set to Enable VPN, which specifies whether the BlackBerry VPN client is turned on. (30)
- Enable/disable policy for mobile networks, Wi-Fi, GPS, FM radio, Bluetooth, NFC – an IT policy rule may be set to enable or disable mobile networks, Wi-Fi, GPS, FM radio Bluetooth or NFC. (31)
- Enable/disable policy for data signaling over USB, SD card, HDMI – an IT policy rule may be set to enable or disable the use of USB, SD card or HDMI interfaces. (32)
- Enable/disable policy for data transfer capabilities – an IT policy rule may be set to enable or disable the use of Media sharing, Miracase, BlackBerry Bridge, Wi-Fi hotspot, or Bluetooth. (33)
- Enable/disable policy for developer modes – an IT policy rule may be set to restrict or allow development mode for BlackBerry device users. Development mode allows software development tools to connect to a device and also allows administrators or users to install applications directly on the device using a USB or Wi-Fi connection. If 'Restrict development mode' is selected, users can only download and install applications from the BlackBerry World storefront, and administrators can send applications to devices using the management console. (34)
- Enable/disable policy for data at rest protection – an IT policy rule may be set to enable or disable the protection of data at rest for work space and personal space. (35)
- Enable policy for removable media's data at rest protection – an IT policy rule may be set to specify the level of file system encryption that the BlackBerry device uses to encrypt files that it stores on an external file system. This IT policy rule may be used to require the BlackBerry device to encrypt an external file system, either including or excluding multi-media directories. (36)
- Enable/disable policy for local authentication bypass – an IT policy may be set to bypass authentication for some phone functions, not including the work space. (37)
- Bluetooth trusted channel policy – an IT policy may be set to configure the Bluetooth policy to allow or disallow Bluetooth discoverable mode, allow or disallow connections based on Bluetooth version (1.0, 1.1, 1.2 and 2.0) and create a Bluetooth profile to dictate the limitations on the use of Bluetooth connections. (38)
- Enable/disable policy for display notification – an IT policy may be set to specify when to display notifications on the external display. The options are Never, Always, Only when unlocked. There is no capability for other applications to perform notifications of this type. (39)

- Policy for establishing a trusted channel – The security policy may be set to permit or deny the establishment of a trusted channel if the certificate validity cannot be verified. (40)
- Certificate used to validate digital signatures on applications - The Administrator is able to configure the certificate used to validate digital signatures associated with mobile applications. (43)
- Unlock banner policy – an IT policy may be set for 'Display organization notice after device restart'. This is used to specify whether a BlackBerry device displays the organization notice that was assigned to a device profile each time a user restarts the device. If this rule is selected, after the user restarts the device, the organization notice appears before the user is prompted for the device password. (46)
- Configure the auditable items - An Administrator may configure which items are to be audited within the event logging, info event logging, warning event logging, error event logging, successful event logging and failure event logging functions.(47)
- Enable/Disable USB mass storage mode – The use of USB mass storage may be disabled through use of an IT Policy, as follows:
    - Allow USB On-The-Go (OTG) mass storage. This policy may be used to specify whether a user can use the USB OTG feature and connect USB mass storage devices (such as USB sticks) to a BlackBerry device. If this rule is not selected, the user cannot connect USB mass storage devices to it.
    - Allow computer to access device. This policy may be used to specify whether a computer can access content on a BlackBerry device using a USB connection or the file-sharing option with a Wi-Fi connection. If this rule is not selected, the computer cannot access content on the device using a USB or Wi-Fi connection and the device can't share media content with Digital Living Network Alliance (DLNA) Certified devices. (48)
- Enable/Disable backup – Data may be backed up locally to a USB device. IT policy may be implemented to enable or disable this functionality. Remote backup is not supported, and is therefore always disabled. (49)
- Enable/Disable location services – Location services may be enabled/disabled for the device. (51)
- Enable/Disable policy for user unenrollment – A device may be deactivated by an Administrator, essentially disenrolling the device in management. User self-unenrollment may be prevented by policy.(52)
- Enable/Disable automatic transfer of diagnostic data - Diagnostic data originating at the Mobile Device may be sent to wireless service providers. This functionality may be enabled or disabled.(53a)
- Full wipe of all user data and applications – An administrator may choose to wipe an entire device. (53d)

TOE Security Functional Requirements addressed: FMT_SMF.1(1)

7.4.5 Specification of management functions (Server configuration of server)

The BES12 provides functionality to allow administrators to manage the certificates used by the server.

Administrative steps must be taken to set up devices for activation. Using user accounts, user groups, and device groups, the MDM Server may configure the devices allowed to be enrolled. The activation settings may be used to limit the time period allowed for enrollment.

The BES Administrator may configure the banner that appears when a device is locked.

The BES Administrator may configure how often commands are sent to the agent to:

- Query connectivity
- Query the version of the mobile device software
- Query the version of the mobile device hardware
- Query the version of installed applications
- Read audit records maintained by the mobile device.

The BES Administrator may retrieve audit records from the mobile device. These records may be transferred to another server.

TOE Security Functional Requirements addressed: FMT_SMF.1(2)

7.4.6 Security management roles

Administrator roles specify the information that an administrator can view and the tasks that an administrator can perform in the BES12. Each role consists of a set of permissions that are assigned to an administrator account. The BES12 includes preconfigured roles. The following customized roles shall be created by an administrator when the TOE is used in the evaluated configuration:

- Server primary administrator:
    - This role is configured such that users in this role may be responsible for server installation, initial configuration, and maintenance functions. They may be responsible for the setup and maintenance of Security configuration administrator and Auditor accounts.
- Security configuration administrator:
    - This role is configured such that users in this role may be responsible for security configuration of the server, setting up and maintenance of mobile device security policies, defining device user groups, setup and maintenance of device user group administrator accounts, and defining privileges of device user group administrators.
- Device user group administrator:

  - This role is configured such that users in this role may be responsible for maintenance of mobile device accounts, including setup, change of account configurations, and account deletion. These users may only perform administrative functions assigned by the Security configuration administrator.

- Auditor:
  - This role is configured such that users in this role may be responsible for reviewing and maintaining server and mobile device audit logs.

The 'Administrator' role (which is also called 'Security Administrator' in the guidance documentation) has permissions to perform all tasks in the BES12.

The Mobile Device User role has no permissions on the BES, but may perform any task allowed by the IT policy rules on the user's own device.

TOE Security Functional Requirements addressed: FMT_SMR.1(1)

7.5 PROTECTION OF THE TSF

7.5.1 Self tests

7.5.1.1 MDM Server Self tests

The TOE performs self-tests on its cryptographic functionality and integrity validation on TSF software on start up. If one of these tests fails to complete, the TOE does not boot and thus transitions to a non-operational state.

Known Answer Tests (KATs) are performed on the cryptographic functions implemented in the cryptographic module, including those that are not implemented in the TSF. This includes KATs are performed on Triple-DES, AES, SHA (via HMAC-SHS), HMAC-SHS, RNG, RSA Signature Algorithm, Diffie-Hellman, Elliptic Curve Diffie-Hellman, ECMQV, and KDF (via key agreement). For DSA and ECDSA, Pair-wise Consistency Test is used. Any failure of a KAT is a critical failure.

The software integrity test deploys ECDSA signature validation to verify the integrity of the cryptographic module. Failure of the integrity test is a critical failure.

Self-test failure places the cryptographic module in the Error state, wherein no cryptographic operations can be performed. If any self-test fails, the cryptographic module produces an error code and enters the Error state. The BES software does not start.

Additionally, a Continuous RNG Test is executed on all RNG generated data, examining the first 160 bits of each requested random generation for repetition. This ensures that the RNG is not stuck at any constant value. Also, upon each generation of a RSA, DSA, or ECDSA key pair, the generated key pair is tested for correctness by generating a signature and verifying the signature on a given message as a Pair-wise Consistency Test. Upon generation or reception of an Elliptic Curve Diffie-Hellman key pair, the key pair is tested for correctness by checking shared secret matching of two key agreement parties as a Pair-wise Consistency Test.

Self-tests are also performed on TOE executables. The manifest file includes an AES 256 CMAC hash of the executables. The manifest file itself is signed using the BlackBerry signing key, and BES is delivered with the corresponding public key. On startup, the signature on the manifest file is verified. Hashes are created on the TOE executables and compared with the hash values found in the manifest file. If the hash value comparison fails, BES will not start.**TOE Security Functional Requirements addressed**: FPT_TST_EXT.1(1).

7.5.2 Trusted update

7.5.2.1 Update of MDM Server

The current version of the MDM server software can be queried from the Windows Server operating system on which the BES is installed. This is done by going to Control Panel > Programs > Programs and Features and selecting BES12. The version, including the build number, can be found under 'Version'.

Each software upgrade for the BES is packaged in the Java Archive (JAR) format. The JAR file is signed with the private key of the BlackBerry Build system using SHA256withRSA with a 256 byte (2048 bit) code signing key. When an administrator installs a software upgrade, the software is verified prior to installation. For each software update, the following steps are performed:

1. BlackBerry Build system generates a JAR file containing the required files for installation;
2. BlackBerry Build system signs the JAR file with the private key corresponding to the public key in the BlackBerry X.509 certificate;
3. The BES Administrator contacts BlackBerry to request the signed JAR file;
4. The BES Administrator executes a BES command (UpdateVerification) to validate and extract the file, as follows:
    a. The signature on the JAR file is validated using the public key from the BlackBerry X.509 certificate,
    b. Contents of the JAR file are validated to ensure that no modifications or additions have been made to the file,
    c. Results of the validation are logged to the security logs, and
    d. Extraction does not proceed unless the signature verification is successful;
5. If validation passes, the BES Administrator then executes the extracted Setup.exe file;
6. The details of the signing certificate are displayed by the Windows operating system. The BES Administrator verifies that the details of this certificate are correct; and
7. The BES Administrator completes the installation as described in the BES Administration Guide.

TOE Security Functional Requirements addressed: FPT_TUD_EXT.1.

7.6 TOE ACCESS

An administrator may configure a login notice to display whenever an administrator accesses the management console. The notice is configurable, and informs the administrator or user about the terms and conditions involved with using the interface. When configured to display, the administrator or user must click 'OK' before being allowed to log in.

TOE Security Functional Requirements addressed: FTA_TAB.1.

7.7 TRUSTED PATH / CHANNELS

7.7.1 Inter-TSF Trusted channel (Authorized IT Entities)

TLS is used to support a trusted channel between the MDM Server and an audit server, and between the MDM Server and an authentication server.

TOE Security Functional Requirements addressed: FTP_ITC.1(1).

7.7.2 Inter-TSF Trusted channel (MDM Agent)

When BES12 sends device management data such as IT policies, profiles, or IT administration commands and required apps from the organization's network to BlackBerry 10 devices, it always sends the data through the organization’s own Wi-Fi network or VPN.

To protect data in transit between BES12 and an enrolled device, a mutually authenticated TLS connection is established over a Wi-Fi or VPN link provided by the organization. Authentication is established using the certificates that were provisioned at the time of enrollment. This trusted path is used to send device management policies and commands to the enrolled device.

TOE Security Functional Requirements addressed: FTP_ITC.1(2).

7.7.3 Trusted path for remote administration

An administrator communicates with the BES over an HTTP/TLS protected link. The administrator identifies the end point by selecting the correct web address for the BES administrative interface. The BES identifies the administrator through username and password. All administrative sessions are initiated by the administrator. The TLS protocol provides protection from disclosure, and provides detection of any modification of the communicated data.

TOE Security Functional Requirements addressed: FTP_TRP.1(1).

7.7.4 Trusted path for enrolment

To protect data in transit between BES12 and a device being enrolled, a mutually authenticated TLS connection is established over a Wi-Fi or VPN link provided by the organization. Authentication is initially provided using a username and password. An http connection is made initially to perform user authentication using username and password. The device then sends a certificate signing request, which is then answered with a certificate. Then a mutually authenticated TLS connection is established. The trusted path is then

used to complete the enrollment and send device management policies and commands to the enrolled device.

TOE Security Functional Requirements addressed: FTP_TRP.1(2).

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Critical Failure	Any failure that causes the BES software to fail to start is a critical failure. A failure may be any error that results in the creation of an audit log, but allows the software to continue operation.
MDM Agent	The MDM Agent is installed on the mobile device as an application or as part of the mobile device's operating system. It is responsible, with the MDM Agent platform, for enforcing the SFRs on the mobile device.
MDM Server	The MDM Server is an application on a general-purpose platform or on a network device that executes in a trusted network environment. It is responsible for managing device enrollment, configuring and sending policies to the MDM Agents, collecting reports on device status and sending commands to the MDM Agents.
Work space	The BlackBerry 10 OS isolates the work file system and work applications from the personal file system and personal applications, and allows for policies that provide added protection for the work files and applications. These are known as the work space.

Table 26 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
BAR	BlackBerry Archive
BBI	BlackBerry Infrastructure
BES	BlackBerry Enterprise Service
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with CBC-Message Authentication Code

Acronym	Definition
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMC	Certificate Management over Cryptographic Message Syntax
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTR	Counter
DH	Diffie-Hellman
DLNA	Digital Living Network Alliance
DN	Distinguished Name
DNS	Domain Name System
DRBG	Deterministic Random Bit Generation
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security
EC	Elliptic Curve
EC-SPEKE	Elliptic Curve Simple Password Exponential Key Exchange
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Key Exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMA	Enterprise Management Agent
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
FM	Frequency Modulation
GCM	Galois Counter Mode
GPS	Global Positioning System
HDMI	High-Definition Multimedia Interface
HMAC	Hash Message Authentication Code

Acronym	Definition
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IPSec	Internet Protocol Security
IP	Internet Protocol
IT	Information Technology
IV	Initialization Vector
KAT	Known Answer Test
KDF	Key Derivation Function
KW	Key Wrap
KWP	Key Wrap with Padding
LDAP	Lightweight Directory Access Protocol
MD	Mobile Device
MDM	Mobile Device Management
MDM PP	Protection Profile for Mobile Device Management v.2.0
NFC	Near Field Communication
NIAP	National Information Assurance Partnership (US)
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OE	Operating Environment
OFB	Output Feedback
OID	Object Identifier
OS	Operating system
OSP	Organization Security Policy
OTG	On-The-Go
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
RA	Registration Authority
RBG	Random Bit Generator
RFC	Request for Comment
RNG	Random Number Generator

Acronym	Definition
RSA	Rivest, Shamir and Adleman
SAN	Subject Alternative Name
SCEP	Simple Certificate Enrollment Protocol
SD	Secure Digital
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SRP	Server Routing Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

Table 27 – Acronyms

ANNEX A

The following table provides a listing of all of the auditable events and the corresponding audit requirement. The table also includes sample data to show the content of the logs.

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
FAU_ALT_EXT.1	Type of alert								
FAU_GEN.1(1)	Start-up and shutdown of the MDM Server software	2018-01-15 19:35:13:220 UTC	Server started	NA	bc-dcoultis10.core2.sqm.testnet.rim.net	System	NA	TRUE	Component=Core
FAU_GEN.1(1)	Start-up and shutdown of the MDM Server software	2018-01-15 19:35:13:220 UTC	Server stopped	NA	bc-dcoultis10.core2.sqm.testnet.rim.net	System	NA	TRUE	Component=Core
FAU_GEN.1(1)	Commands issued from the MDM Server to an MDM Agent	2018-01-15 19:35:13:220 UTC	Command delivered	aa3dc6e6-210a-4d4e-9b7b-e50b0235fe8f	bc-dcoultis05.core2.sqm.testnet.rim.net	dc@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Command Type=WORKSPACE_LOCK_SETPASSWORD
FAU_GEN.1(1)	Commands issued from the MDM Server to an MDM Agent	2018-01-15 19:35:13:220 UTC	Command sent	25d3c8d8-709a-40ce-ad53-918798368ca4	bc-dcoultis05.core2.sqm.testnet.rim.net	dc@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Command Type=WORKSPACE_LOCK_SETPASSWORD
FCS_CKM.1	Failure of key generation activity for authentication keys	2018-01-15 19:35:13:220 UTC	Key Generated	84c77c89-492a-43cb-8d54-a0bb6eb31b23	bc-dcoultis05.core2.sqm.testnet.rim.net	admin	BCOP1065	FALSE	Message Description=Type:[Alert] Time stamp:[Mon Jan 15 13:20:30 EST 2018] IP:[unknown] Certificates:[] Description:[FATAL Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was received. TLSState: Key Exchange Alert.]

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
FCS_HTTPS_EXT.1	Failure of the certificate validity check	2016-12-02 16:31:00:150 UTC	Certificate validated		bc-dcoultis05.core2.sqm.testnet.rim.net	System		FALSE	Message Description=certificate chain failed validation:leaf certificate has invalid basicContraints.isCA=true;
FCS_RBG_EXT.1	Failure of the randomization process	2016-12-02 16:31:00:150 UTC	Randomization initialized	03b508d9-5a1d-4eb5-8fa2-4b9a144b614f	bc-dcoultis08.core2.sqm.testnet.rim.net	System	BCOP1500	FALSE	Message Description=randomization failure
FCS_TLSC_EXT.1	Failure to establish a TLS session. Failure to verify presented identifier	2016-12-02 16:31:00:150 UTC	Certificate validated		bc-dcoultis05.core2.sqm.testnet.rim.net	System		FALSE	Message Description=Type:[Alert] Time stamp:[Mon Jan 15 13:20:30 EST 2018] IP:[unknown] Certificates:[] Description:[FATAL Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was received. TLSState: Key Exchange Alert.]
FCS_TLSS_EXT.1	Failure to establish a TLS session	2016-12-02 16:31:00:150 UTC	Certificate validated						Message Description=Type:[Alert] Time stamp:[Mon Jan 15 15:46:54 EST 2018] IP:[null:-1] Certificates:[] Description:[FATAL Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was received. TLSState: Key Exchange Alert.]
FIA_ENR_EXT.1	Failure of MD user authentication	2016-12-02 16:31:00:150 UTC	Device enrollment started	8e3ab9a8-7bbd-445a-8efa-e74b6f56351c	bc-dcoultis05.core2.sqm.testnet.rim.net	system	BCOP1065	FALSE	Enrollment username=dxc;Message Description=No user was found for tenant Id 1, and username = dxc
FIA_X509_EXT.1	Failure to validate X.509 certificate	2016-12-02 16:31:00:150 UTC	Certificate validated						

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
FIA_X509_EXT.2	Failure to establish connection to determine revocation status		Certificate validated		bc-dcoultis05.core2.sqm.testnet.rim.net	system		FALSE	Message Description=Failed OCSP revocation check for certificate:O=BDMI Device Client, OU=BCOP1065, CN=611dc1d8-1623-4aa9-abc4-0588b09a2f7b;
FMT_MOF.1(1)	Issuance of command to perform function. Change of policy settings	2018-01-15 19:35:13:220 UTC	Policy sent	404782e3-6603-4375-85f7-bb6a364c3c61	bc-dcoultis05.core2.sqm.testnet.rim.net	dx@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB
		2018-01-15 19:35:13:220 UTC	Policy delivered	20682c8b-69ef-403a-8628-cfebe239e966	bc-dcoultis05.core2.sqm.testnet.rim.net	dx@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Policy Description=VPN Profile;Payload=<?xml version="1.0" encoding="UTF-8" standalone="yes"?><communications signature="Zpgy/TvScxtR6mc0lc/FlFUgSU0=" xmlns="dto.v1.mdm.rim.com"><communication signature="Ed7RyZfcQFyNPsS4nOXAT8BeuM8="><groupId>dc1</groupId><items><item><itemId>22</itemId><booleanValue><value>false</value></booleanValue></item><item><itemId>36</itemId><stringValue><value>0</value></stringValue></item><item><itemId>6</itemId><integerValue><value>0</value></integerValue></item><item><itemId>33</itemId><stringValue><value>other</value></stringValue></item><item><itemId>28</itemId><booleanValue><value>true</value></booleanValue></item><item><itemId>3</itemId><integerValue><value>3</value></integerValue></item><item><itemId>15</itemId><booleanValue><value>true</value></booleanValue></item><item><itemId>1</itemId><stringValue><value>dc1</value></stringValue></item><item><itemId>2</itemId><booleanValue><value>false</value></booleanValue></item><item><itemId>34</itemId><stringValue><value>startup</value></stringValue></item><item><itemId>29</itemId><integerValue><value>0</value></integerValue></item><item><itemId>14</itemId><integerValue><value>0</value></integerValue></item><item><itemId>4</itemId><integerValue><value>1</value></integerValue></item></items><type>1</type></communication></communications>

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
		2018-01-15 19:35:13:220 UTC	Policy delivered	73931bda-d1eb-4106-9cad-1febe656095f	bc-dcoultis05.core2.sqm.testnet.rim.net	dx@x.ca	BCOP1065	FALSE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Policy Description=Wi-Fi Profile;Message Description=WiFi_Configuration_Failure;Payload=<?xml version="1.0" encoding="UTF-8" standalone="yes"?><communications signature="Ew9jBJ7cKIjsRdSkNShgScSof7s=" xmlns="dto.v1.mdm.rim.com"><communication signature="Ed7RyZfcQFyNPsS4nOXAT8BeuM8="><groupId>dc1</groupId><items><item><itemId>22</itemId><booleanValue><value>false</value></booleanValue></item><item><itemId>36</itemId><stringValue><value>0</value></stringValue></item><item><itemId>6</itemId><integerValue><value>0</value></integerValue></item><item><itemId>33</itemId><stringValue><value>other</value></stringValue></item><item><itemId>28</itemId><booleanValue><value>true</value></booleanValue></item><item><itemId>3</itemId><integerValue><value>3</value></integerValue></item><item><itemId>15</itemId><booleanValue><value>true</value></booleanValue></item><item><itemId>1</itemId><stringValue><value>dc1</value></stringValue></item><item><itemId>2</itemId><booleanValue><value>false</value></booleanValue></item><item><itemId>34</itemId><stringValue><value>startup</value></stringValue></item><item><itemId>29</itemId><integerValue><value>0</value></integerValue></item><item><itemId>14</itemId><integerValue><value>0</value></integerValue></item><item><itemId>4</itemId><integerValue><value>1</value></integerValue></item></items><type>1</type></communication><communication signature="uX0vuFHmPgPdTLg/vXV0k6WirLo="><groupId>dc2</groupId><items><item><itemId>22</itemId><booleanValue><value>false</value></booleanValue></item><item><itemId>36</itemId><stringValue><value>0</value></stringValue></item><item><itemId>6</itemId><integerValue><value>0</value></integerValue></item><item><itemId>33</itemId><stringValue><value>other</value></stringValue></item><item><itemId>28</itemId><booleanValue><value>true</value></booleanValue></item><item><itemId>3</itemId><integerValue><value>3</value></integerValue></item><item><itemId>15</itemId><booleanValue><value>true</value></booleanValue></item><item><itemId>1</itemId><stringValue><value>dc1</value></stringValue></item><item><itemId>2</itemId><booleanValue><value>false</value></booleanValue></item><item><ite

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
									mId>34</itemId><stringValue><value>startup</value></stringValue></item><item><itemId>29</itemId><integerValue><value>0</value></integerValue></item><item><itemId>14</itemId><integerValue><value>0</value></integerValue></item><item><itemId>4</itemId><integerValue><value>1</value></integerValue></item></items><type>1</type></communication></communications>
		2018-01-15 19:35:13:220 UTC	Command sent	86ef6ea6-d6c8-434f-9a5a-c38088cd6a8f	bc-dcoultis05.core2.sqm.testnet.rim.net	dx@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Command Type=WORKSPACE_LOCK_SETPASSWORD
		2018-01-15 19:35:13:220 UTC	Command delivered	deaf6579-af37-4f38-9f28-db2f0a4f17e3	bc-dcoultis05.core2.sqm.testnet.rim.net	dx@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Command Type=WORKSPACE_LOCK_SETPASSWORD
FMT_MOF.1(2)	Enrollment	2018-01-15 19:35:13:220 UTC	Device enrollment started	1803dac5-0ac6-4e08-954d-c3035ee41d2b	bc-dcoultis05.core2.sqm.testnet.rim.net	dc@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB
		2018-01-15 19:35:13:220 UTC	Device enrollment completed	f01556e5-f9f6-43dc-b2ed-1f0a098d489c	bc-dcoultis05.core2.sqm.testnet.rim.net	dc@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB
FMT_SMF.1(2)	Success or failure of function	2018-01-15 19:35:13:220 UTC	Device enrollment completed	1811f2cd-be87-4354-a00a-c1b01e655e8a	bc-dcoultis05.core2.sqm.testnet.rim.net	dx@x.ca	BCOP1065	FALSE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB;Message Description=Code: User_Cancel Description: User did not accept BlackBerry disclaimer; enrollment was cancelled.
FPT_TST_EXT.1	Initiation of self-test	2018-01-15 19:35:13:220 UTC	Self Test Initiated	257254fb-d7b2-41d3-804c-9be59725aae3	bc-dcoultis05.core2.sqm.testnet.rim.net	system		TRUE	Self Test Initiated, Success, Component=Core
	Failure of self-test. Detected integrity violation	2018-01-15 19:35:13:220 UTC	Self Test Completed	257254fb-d7b2-41d3-804c-9be59725aae3	bc-dcoultis05.core2.sqm.testnet.rim.net	system		FALSE	Self Test Completed, Failed, Component=Core, Reason=Hash 504b697dfe5a1061065a4ba3ed8d5df68680abecf3b814886eb45ef7ccc05ccc, ba25cbfe92a310707ed1697012ffa3fbf32aeec16d49c58bcba68f9adfba1b7a for Core/tomcat-core/lib/postgresql.jar does not match.

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
FPT_TUD_EXT.1	Success or failure of signature verification								
FTA_TAB.1	Change in banner setting		Access banner modified	ee596fee-9f63-40c1-bcfe-454e57852198	bc-dcoultis05.core2.sqm.testnet.rim.net	admin	BCOP1065	TRUE	Access banner admin banner enabled=true;Access banner admin banner value=Content goes here
FTP_ITC.1(1)	Initiation and termination of the trusted channel	2018-01-15 19:35:13:220 UTC	Connection with external service established	e1bb03b5-cae3-4591-8823-efbcaf8ea57e	bc-dcoultis05.core2.sqm.testnet.rim.net	system		TRUE	Trusted Channel Protocol=TLS;Non-TOE Endpoint Name=Management console;Non-TOE Endpoint URL=https://localhost:8448/status
		2018-01-15 19:35:13:220 UTC	Connection with external service terminated	e1bb03b5-cae3-4591-8823-efbcaf8ea57e	bc-dcoultis05.core2.sqm.testnet.rim.net	system		TRUE	Trusted Channel Protocol=TLS;Non-TOE Endpoint Name=Management console;Non-TOE Endpoint URL=https://localhost:8448/status
FTP_ITC.1(2)	Initiation and termination of the trusted channel	2018-01-15 19:35:13:220 UTC	Connection with device established		bc-dcoultis05.core2.sqm.testnet.rim.net	device	BCOP1065	TRUE	Trusted Channel Protocol=TLS;Identify of Initiator=430d88a0-9c58-47f9-aacf-1fdcd2bb50e3;Identify of Recipient=bc-dcoultis05.core2.sqm.testnet.rim.net
		2018-01-15 19:35:13:220 UTC	Connection with device terminated		bc-dcoultis05.core2.sqm.testnet.rim.net	system	BCOP1065	TRUE	Trusted Channel Protocol=TLS;Identify of Initiator=bc-dcoultis05.core2.sqm.testnet.rim.net;Identify of Recipient=430d88a0-9c58-47f9-aacf-1fdcd2bb50e3
FTP_TRP.1(1)	Initiation and termination of the trusted channel	2018-01-15 19:35:13:220 UTC	User logged in	fbe93c34-4e8c-47e8-9564-451d9fd2a9cd	bc-dcoultis05.core2.sqm.testnet.rim.net	admin	BCOP1065	TRUE	Trusted Channel Protocol=TLS;Identify of Administrator=admin
		2018-01-15 19:35:13:220 UTC	User logged out	60775fb9-a53b-4820-826b-a3d44c71f6e2	bc-dcoultis05.core2.sqm.testnet.rim.net	System		TRUE	Trusted Channel Protocol=TLS;Identify of Administrator=admin
FTP_TRP.1(2)	Initiation and termination of the trusted channel	2018-01-15 19:35:13:220 UTC	Connection with device established		bc-dcoultis05.core2.sqm.testnet.rim.net	device	BCOP1065	TRUE	Trusted Channel Protocol=TLS;Identify of Initiator=430d88a0-9c58-47f9-aacf-1fdcd2bb50e3;Identify of Recipient=bc-dcoultis05.core2.sqm.testnet.rim.net
		2018-01-15 19:35:13:220 UTC	Connection with device terminated		bc-dcoultis05.core2.sqm.testnet.rim.net	system	BCOP1065	TRUE	Trusted Channel Protocol=TLS;Identify of Initiator=bc-dcoultis05.core2.sqm.testnet.rim.net;Identify of Recipient=430d88a0-9c58-47f9-aacf-1fdcd2bb50e3

Requirement	Auditable Event	Date created	Event	Correlation ID	Host	User	Tenant	Success	Details
	Certificate signing request completed	2018-01-15 19:35:13:220 UTC	Certificate signing request completed	1803dac5-0ac6-4e08-954d-c3035ee41d2b	bc-dcoultis05.core2.sqm.testnet.rim.net	system	NULL	TRUE	Certificate Signing Request Algorithm=ECC;Certificate Signing Request Subject=CommonName=2ABB3DC6;Certificate Subject=CN=e5c28ebb-8472-4395-8e82-70faa535e41b, OU=BCOP1065, O=BDMI Device Client;Certificate Issuer=CN=BlackBerry Enterprise Server ECC Intermediate CA 1, OU=BlackBerry Enterprise Service, O=BlackBerry Limited, C=CA
	Device unenrolled	2018-01-15 19:35:13:220 UTC	Device unenrolled	f8c4b315-0915-4c83-b585-75a2ec37765d	bc-dcoultis05.core2.sqm.testnet.rim.net	dc@x.ca	BCOP1065	TRUE	User Identity=dc@x.ca;Device Identity=2ABB3DC6;Device OS Family=BB

Table 28 – List of Auditable Events

Administrative Actions (Command or Policy records contain Command Name, DeviceUser, and DeviceID, in addition to the details shown in Table 29.

Record ID	Date created	Category	Event	Correlation ID	Host	User	Success	Details
1	2017-12-14 14:59:36:957 UTC	System Access	Self Test Initiated	2e5f83ef-b68e-4574-a298-e563510ebf4a	bc-dcoultis08.core2.sqm.testnet.rim.net	system	TRUE	Self Test Initiated, Success, Component=Core
2	2017-12-14 14:59:37:487 UTC	System Access	Self Test Completed	2e5f83ef-b68e-4574-a298-e563510ebf4a	bc-dcoultis08.core2.sqm.testnet.rim.net	system	TRUE	Self Test Completed, Success, Component=Core
	2018-01-15 15:32:20:363 UTC	System Settings	Security audit settings modified	e76157a6-85b8-48ea-bdf8-cf0ab67ba7f0	bc-dcoultis05.core2.sqm.testnet.rim.net	admin	TRUE	Setting Changes="DailyPurge=00:00:00Z";Event Changes="Device enrollment started=On,Policy sent=OnSuccess,Command sent=OnSuccess,Server started=OnSuccess,Presented Identifier Verification=OnFailure,Authentication of service API request=OnFailure,Connection with device established=OnSuccess,Connection with external service established=OnSuccess,Access banner modified=OnSuccess,Command delivered=On,Device enrollment completed=On,Key generated=OnFailure,Certificate validated=OnFailure,Server stopped=OnSuccess,Randomization initialized=OnFailure,Policy delivered=On,Device unenrolled=OnSuccess,Connection with device terminated=OnSuccess,Connection with external service terminated=OnSuccess,Certificate signing request completed=On"

Table 29 – Audit of Administrative Events