Security Target for BlackBerry UEM Server

Version 1.9

2025-08-18

BlackBerry

12.21.1 (40.32.0)

Revision	Date	Description
0.1	2023-08-04	NN, initial draft version for review
0.2	2023-09-11	Update based on BlackBerry comments
0.3	2023-10-10	Update based on BlackBerry input
0.4	2023-10-24	Update based on BlackBerry input
0.5	2023-11-16	Update based on BlackBerry comments
0.6	2023-11-16	Release version
0.7	2024-04-18	Update based on evaluator and BSI comments
0.8	2024-05-08	Further updates based on evaluator and BlackBerry comments
0.9	2024-09-23	Update based on consultancy work
1.0	2024-12-13	Include Samsung Knox and certificate pinning for iOS
1.1	2025-03-13	All changes have been accepted, added UEM version, deleted comments, and making PDF based on evaluator Stephan request. Added Micro Architecture level information and Windows 19,22 alignment based on AGD, requested by evaluator Daniel and Michael
1.2	2025-03-14	Updated Cipher suites as discussed in sections FTP_PRO.1.6 and 7.7, additionally removed DHE key reference within 7.7 based on evaluators comment
1.3	2025-03-19	Updated hardware requirement in section 1.5.5
1.4	2025-03-25	Updated 7.2 SF.Crypto – Cryptographic support
1.5	2025-04-03	Update based on evaluator comments
1.6	2025-04-15	Updated table 12
1.7	2025-05-05	Addressed BSI jailbreak Apple OS removal comment
1.8	2025-05-19	Update based on evaluator comments
1.9	2025-08-18	Updated version number i.e. 40.32.0

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Security Target reference and organisation

Title:	Security Target for BlackBerry UEM Server
ST Version:	1.9
Status:	To Release
Date:	2025-08-18
Keywords:	Mobile Device Management, MDM Server

This Security Target (ST) follows the structure as defined in [CC:2022] Part 1. For this ST introduction, security problem definition, security objectives, security requirements, TOE summary specification, references and abbreviations have been defined as the main sections.

The introduction consists of the following sections:

- Security Target reference and organisation
- TOE Reference
- TOE Overview
- Terms and Definitions
- TOE description.

The security problem definition comprises threats, organisational security policies and assumptions. It defines the security aspects for the environment for the TOE.

The security objectives reflect the stated intent of the ST. They pertain to how the TOE will counter identified threats and how it will cover identified organisational security policies and assumptions. The security objectives are divided into security objectives for the TOE and for the environment. The security objectives rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security problem definition and that they are suitable to cover them.

All extended security requirements that are not contained in Part 2 of [CC:2022] are defined in the extended components section.

The security requirements section provides detailed requirements, in separate subsections, for the TOE and its environment. The security requirements are further divided into the TOE security functional requirements and the TOE security assurance requirements.

The security functions provided by the TOE are described in the TOE summary specification. This section also maps the TOE security functions to the security functional requirements that are used in this ST.

The document is concluded by the references and abbreviations sections.

1.2 TOE Reference

The TOE is BlackBerry UEM Server version 12.21.1 (40.32.0)

1.3 TOE Overview

Mobile Device Management (MDM) is the centralised management of mobile devices such as smartphones, tablets, and notebooks that are used in an organisation. It represents an essential part of Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM) systems.

The purpose of an MDM system is to ensure the security and functionality of mobile devices in accordance with corporate policies as well as to protect the corporate network from unauthorised access.

1.3.1 TOE Type

The TOE is the trusted server of a Mobile Device Management (MDM) system, i.e. the TOE type is *Mobile Device Management – Trusted Server (MDM-TS)*.

The TOE provides services to distribute data, applications, updates, as well as configuration commands and policy settings on mobile devices. Both corporate and personal mobile devices are supported.

The TOE consists of several server components. This ST distinguishes two TOE components, the TOE device server component and the TOE control server component. This separation is introduced in [MDMTSPP] and is implemented by the TOE. It facilitates a clear distinction between the interactions of the TOE at the device interface and at the staff interface.

Remark (separation of TOE components). The separation of TOE device server component and TOE control server component is beneficial for the overall security of mobile device management:

- It is compatible with established multi-layer information security models in the sense that internal services are not accessible from outside. While the TOE control server component is not accessible from mobile devices, it may have direct access to some internal services, e.g. to an internal directory service.
- It prevents mobile devices from accessing internal network segments since the TOE device server component handles all communication with mobile devices. Therefore, adverse actions from mobile devices against any service in internal network segments can be blocked more easily.

PP Application Note (TOE components).[1] The application of this PP is not limited to TOEs that consist of two physically or virtually separated server components. Any component structure may be PP conformant, as long as it enforces a clear separation between device interactions and staff interactions. The PP/ST author should briefly describe the TOE structure in terms of the TOE components and the degree of physical or virtual separation between device interactions and staff interactions.

ST Application Note (TOE components). The TOE structure is described in section 1.5.2 of this ST.

Any client component of the MDM system (such as the UEM Android Client, UEM iOS Client or Apple's MDM Client) is outside of the TOE boundary.

1.3.2 Usage and Major Security Features

The TOE device server component interacts with mobile devices and is connected to some supporting non-TOE services, in particular enrolment, notification, inventory, database, directory services and logging services. The TOE device server component is directly accessible from any authorised device agent. Communication with device agents consists of the execution of mobile device management functions. The TOE device server component does not directly communicate with staff agents. Any communication with staff agents is performed indirectly by exchanging specific requests with the TOE control server component.

The TOE control server component interacts with staff agents in several roles and is connected to some supporting non-TOE services, in particular the database for retrieving its initial configuration.

[1] Application notes adopted from [MDMTSPP] are labelled as "PP Application Notes". Application notes adopted from [TCCPPM] are labelled as "PPM Application Notes". ST application notes are simply noted as "ST Application Notes".

The TOE control server component is directly accessible from any authorised staff agent. Communication with staff agents consists of several TOE management functions and the initiation of mobile device management functions. The TOE control server component does not directly communicate with device agents. Any communication with device agents is performed indirectly by exchanging specific requests with the TOE device server component.

Figure 1 (adopted from [MDMTSPP]) illustrates a bird's eye view on a typical MDM Trusted Server and its environment, outlining both separated TOE server components. Each TOE component acts as a server in a typical client-server architecture. The clients of the TOE device server component are authorised device agents. The clients of the TOE control server component are authorised staff agents in several roles (manager, auditor, administrator). All services of the TOE are provided on requests of individual device/staff agents relying on trusted communication channels. Any such request is processed by corresponding device/staff attendants. The communication between both TOE components is performed via protected internal data transfer between device attendants (part of the TOE device server) and manager attendants (part of the TOE control server).

The TOE device server component may run in several parallel instances, e.g. to enable load-balancing or fail-safe redundancy. Similarly, the TOE control server component may run in several parallel instances, e.g. to separate different tenants while sharing a common database service.

PP Application Note (multiple instances of TOE components). If some TOE components can be operated in multiple parallel instances, the PP/ST author should describe, how the secure operation of the TOE is protected in terms of e.g. failure resistance and recovery, state synchronisation, or fault tolerance. Also, the PP/ST author may adequately extend the security problem definition, security objectives and security functional requirements (from classes FPT or FRU) of this PP.

ST Application Note (multiple instances of TOE components). For high-availability configurations, the TOE can be operated in multiple instances, pointing to the same database. The database can also be replicated in such scenarios. Note, however, that high-availability configurations are not in the scope of this ST.

PP Application Note (on-premises operation). The on-premises operation of all TOE components is generally preferred because the responsibility for the security of the operational environment is clearly assigned to the corporate information security management. If some TOE components can be operated off-premises, the PP/ST author should briefly describe how the affected TOE components are to be protected by the operational environment.

ST Application Note (on-premises operation). BlackBerry UEM is available as an on-premises environment and as a cloud service. In the evaluated configuration, the TOE is installed and operated on-premises.

PP Application Note (connection to supporting services). Depending on the operational environment of each TOE component, the PP/ST author should briefly describe how the connection to any supporting service is to be protected by the operational environment.

ST Application Note (connection to supporting services). Connections to supporting services are protected as described in section 1.5.5 of this ST.

PP Application Note (TOE delivery/updates). This PP purposely does not address TOE delivery or TOE updates. The PP/ST author should briefly describe how TOE components are delivered and updated. If the TOE provides specific security features for the secure update of its components, the PP/ST author should adequately extend the security problem definition, security objectives and security functional requirements of this PP.

ST Application Note (TOE delivery/updates). Delivery and update of the TOE is described in section 1.5.6 of this ST.

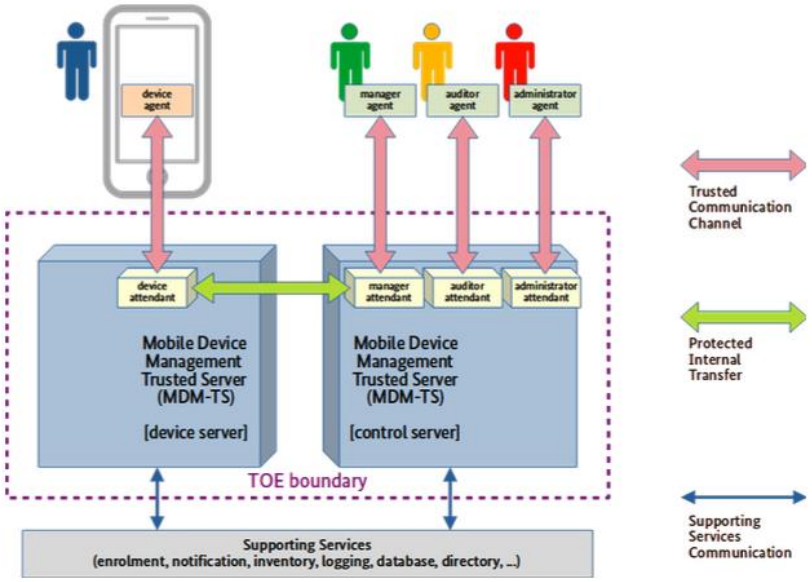

Figure 1: TOE boundary and environment of a typical MDM Server (adopted from [MDMTSPP])

The TOE allows arbitrary grouping of device/staff agents in a very general way. Groupings may be formed for certain characteristics of mobile devices such as vendors, operating systems, etc. Groupings may also be formed for certain organisational structures such as departments, locations etc. The grouping concept is defined in terms of a bounded lattice, i.e., a mathematical structure on partially ordered sets with specific additional properties.

PP Application Note (bounded lattice of groupings). A bounded lattice is a flexible generic structure. It allows different kinds of basic groupings and their combination to tuples of more complex groupings. Some exemplary bounded lattices of groupings are sketched in PP appendix section 1. The PP/ST author should briefly describe the groupings that are supported by the TOE. This PP does not restrict the construction of the bounded lattice in terms of the kind, combination, or complexity of its groupings. However, when the TOE provides multi-tenancy support, the construction should include a bounded sub-lattice of tenant groupings like e.g., in PP appendix section 7.5.

ST Application Note (bounded lattice of groupings).

The TOE provides the following major security features:

- Protected enrolment of mobile devices that are to be managed by the TOE.
- Identification/Authentication of device/staff agents.
- Role-based capabilities and privileges of staff agents.
- Accountability of all services by audit generation and review of device/staff agent interactions.
- Control of MDM activities based on grouping attributes of device/staff agents. The TOE does not provide multi-tenancy support.
- Protection of communication between device attendants (in the TOE device server component) and manager attendants (in the TOE control server component) from disclosure and modification.
- Separation of communication paths for interaction with device agents and staff agents.
- Protection of communication paths and communication channels from disclosure and modification.

- Protection of special categories of user data (PINs, passwords, cryptographic keys/certificates, etc.) from disclosure and modification while it is stored by the TOE.

1.3.3 Non-TOE Hardware/Software/Firmware

PP Application Note (trusted communication channels). If the TOE itself provides trusted communication channels based on cryptographic mechanisms, the PP/ST author should complement this PP with the security problem definition, security objectives and security functional requirements of the PP-Module "Trusted Communication Channel (TCC)" as specified in the PP-Configuration BSI-CC-PP-0116.

ST Application Note (trusted communication channels). The TOE provides trusted communication channels based on cryptographic mechanisms to ensure confidentiality and integrity of data in transit between the TOE and authorised device/staff agents. The TOE does not rely on non-TOE hardware/software for this functionality.

The TOE relies on non-TOE hardware/software for providing a trusted enrolment process of mobile devices to ensure the reliable identification of mobile devices and provisioning of credentials for identification/authentication of device agents. Further details on non-TOE hardware/software/firmware are provided in section 1.5.5.

PP Application Note (device enrolment). This PP purposely does not address any details of the enrolment process of mobile devices. This is because there are various (semi-)automatic enrolment services like Android Zero Touch, Samsung Knox Mobile Enrollment (KME), and Apple Device Enrollment Program (DEP). The MDM Trusted Server may even provide a proprietary trusted enrolment process that could be based, for example, on a two-factor authentication of the human user controlling the mobile device. If the TOE provides specific security features for the device enrolment process, the PP/ST author should adequately extend the security problem definition, security objectives and security functional requirements of this PP.

1.4 Terms and Definitions

administrator agent: a *staff agent* that is associated with the administrator role

administrator attendant: a *staff attendant* that is acting on behalf of requests from an *administrator agent*

auditor agent: a *staff agent* that is associated with the auditor role

auditor attendant: a *staff attendant* that is acting on behalf of requests from an *auditor agent*

bounded lattice: a *lattice* that has a unique least element (bottom, minimum) and a unique greatest element (top, maximum)

cluster of groupings: a security attribute that is associated to *staff agents* and *staff attendants* A cluster of groupings is defined to be a set of *groupings* from a *bounded lattice*.

device agent: an external entity that interacts with the TOE device server component via its device interface

A device agent is an MDM client application running on a mobile device. It may be a generic component of a mobile operation system or a mobile device, or it may be specifically provided by an MDM solution.

device attendant: an active entity in the TOE device server component that performs operations on behalf of requests from an authorised *device agent*

grouping: a security attribute that is associated to *device agents* and *device attendants.* To offer greatest flexibility for the TSF, groupings are structured in a *bounded lattice*

lattice: a mathematical structure that consists of a partial ordering relationship between its elements such that every two elements have a unique greatest lower bound and a unique least upper bound

A lower bound of two elements is an element that is lower than or equal to both elements. The unique greatest lower bound (meet, infimum) is a lower bound that is greater than every other lower bound.

An upper bound of two elements is an element that is greater than or equal to both elements. The unique least upper bound (join, supremum) is an upper bound that is smaller than every other upper bound.

manager agent: a *staff agent* that is associated with the manager role

manager attendant: a *staff attendant* that is acting on behalf of requests from a *manager agent*

staff agent: an external entity that interacts with the TOE control server component via its staff interface

The following types of staff agents are distinguished: *administrator agent*, *auditor agent*, *manager agent*.

A staff agent may be a specifically configured web browser, an application software component, or a web service relay.

staff attendant: an active entity in the TOE control server component that performs operations on behalf of requests from an authorised *staff agent*

The following types of staff attendants are distinguished: *administrator attendant*, *auditor attendant*, *manager attendant*.

1.5 TOE description

1.5.1 Introduction

The BlackBerry Unified Endpoint Management (UEM) Server (TOE) provides centralized management of mobile devices. It is the main part of the BlackBerry UEM product.

1.5.2 TOE Architecture

The UEM Server has two unique components to service staff interactions and device interactions. Both components must be on the same host in the evaluated configuration. Staff members securely interact with the Management console (TOE control server component) via a web browser and the Management console securely communicates with the Core Server component (part of the TOE device server component) to store the results from the staff interactions. Staff can also communicate with the Core Server directly using the BlackBerry Web Services APIs. The Core Server component also communicates with mobile devices in response to the manager's configuration updates.

The TOE device server component and control server component are shown in the figure below. The other components in the figure are not related to the enforcement of any security requirements or are not part of the product, but rather are part of the operational environment.

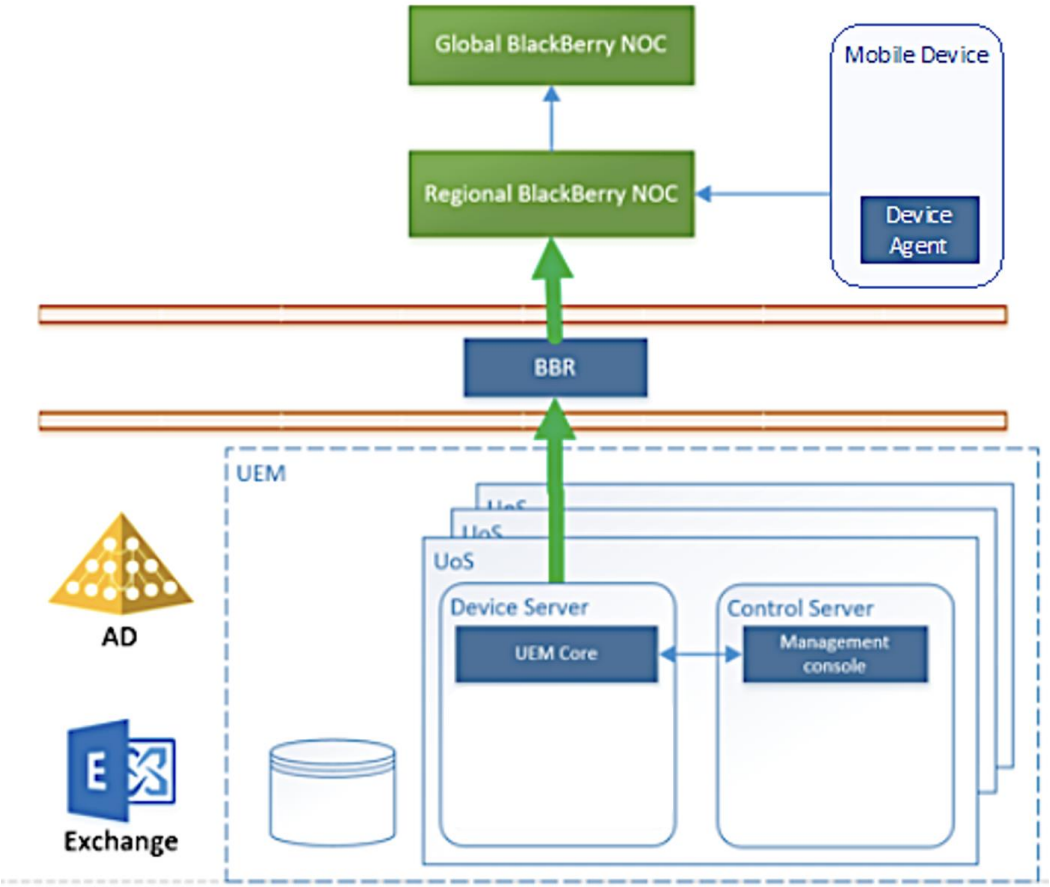

Figure 2: Architecture of the UEM Product

The BlackBerry UEM server is implemented with a combination of Java and native code running on Windows Server 2019 or Windows Server 2022 with Java JRE 17, running in a virtual environment (VMWare ESXi 8.0.2) on an AMD EPYC 7702P 64-Core Processor.

The UEM Server requires a SQL database to operate and must be configured to utilize an LDAP server such as Active Directory (AD) for user authentication as well as optionally a SYSLOG server to export audit records.

Device Server and Control Server form a unit of scale (UoS) This represents the option to have multiple instances of the Device Server and Control Server components for redundancy and high availability. However, this is not in the scope of this ST.

Some other components such as the BlackBerry Enterprise Mobility Server (BEMS) are not included in the scope of evaluation or are not security relevant such as the BlackBerry Router (BBR) and the BlackBerry Network Operations Center (NOC) components. The BlackBerry NOC is a network routing component through which UEM Server – client communication travels. The BlackBerry Router (BBR) can be deployed within a DMZ (demilitarized zone) of a network, to provide additional safeguards in connecting to the BlackBerry NOC. They are not security relevant for the purpose of this evaluation since the server-client channels are secured end to end by encryption keys generated during client enrolment with the UEM Server. Those other components cannot decrypt or otherwise access information in those secure channels, although they can disrupt or redirect them, like any other components on the Internet.

The UEM Server can manage mobile Android devices through interaction with an enrolled UEM Android Client (not part of the TOE) and can manage mobile iOS devices through interaction with the iOS device agent developed by Apple (not part of the TOE).

1.5.3 Physical Scope

The TOE is software only and consists of the BlackBerry UEM server executable, along with the accompanying user guidance listed below.

BlackBerry offers documentation that describes the use and administration of the applicable security features of the TOE. For the purpose of evaluation, the following guides are included in the physical scope of the TOE:

- BlackBerry UEM Administrative Guidance Document, UEM Version 12.21.
- All BlackBerry UEM guides referenced in the Administrative Guidance Document

Certification-specific References
UEM_12.21_MR1_docs.zip contains the full BlackBerry UEM 12.21.1 customer doc set: • Overview and Architecture • Planning Guide • Installation and Upgrade Guide • Configuration Guide • Managing administrators, users, and groups • Managing secure connections • Managing device configurations • Managing email, calendar, and contacts • Managing apps • Activating devices • Monitoring and reporting
• BlackBerry UEM Administrative Guidance Document, UEM Version 12.21
Policy-Reference-Spreadsheet-BlackBerry-UEM.xlsx: The IT policy rule reference spreadsheet for UEM 12.21.1.
The following KB articles are referenced in this document: • KB 52117: How to set up Java when deploying UEM • KB 36470: How to configure network firewalls to work with UEM and BEMS • KB 36596: Antivirus exclusions for UEM
BlackBerry Web Services documentation

Any device agent and any other BlackBerry UEM product component is outside the scope of this evaluation.

1.5.4 Logical Scope

This section summarizes the security functions implemented by the TOE:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels

1.5.4.1 Security audit

The BlackBerry UEM server is designed to generate and export audit events listed in **Table 9**. The audit events are stored in the SQL database and optionally sent to the configured syslog servers as events occur. The BlackBerry UEM server supports TLS tunneling of syslog messages to protect exported audit records.

1.5.4.2 Cryptographic support

The BlackBerry UEM server uses the Certicom Security Builder GSE-J Crypto Core Module for its cryptographic operations. It includes the following algorithms which are applicable for this evaluation:

- AES
- DRBG
- DSA
- ECDSA
- HMAC
- KAS
- RSA
- SHS

The BlackBerry UEM server implements a X.509 key hierarchy summarized as follows:

1) The PKI is rooted in a self-signed certificate (RSA 4096 SHA512) created when the first server is installed.
2) The root is used to issue an intermediate CA certificate (RSA 3072 SHA512) also created when the first server is installed.
3) Additional certificates are issued using the intermediate CA certificate as follows:
   a) Console web server certificate (RSA 3072 SHA512) – used for TLS communication between staff agents (web browser) and TOE
   b) Server certificate (RSA 3072 SHA512) – used for TLS communication between mobile device agents and TOE.
   c) Profile signing certificate (RSA 3072 SHA512)
   d) Per-device BDMI payload signing key (RSA 3072 SHA512)
   e) Per-device enrolled device certificates - issued during enrollment (RSA 3072 SHA512)
4) All of the certificates above, except the per-device certificates, are stored in the SQL database and the key store is AES-GCM-256 encrypted with a DEK also created during installation. The per-device BDMI payload signing keys are encrypted using the DEK

separately from the rest of the key store. The DEK is AES-CBC-256 encrypted using a KEK (a key-encryption-key stored in the Windows key store) that is unique to each unit of scale (created during installation). The encrypted DEK is stored on the local file system of each unit of scale. Integrity of the encrypted DEK is ensured using HMAC-SHA-256 calculated on the encrypted DEK and the associated IV (a separate key used for this hash operation is also stored in the Windows key store) and checked prior to decryption

5) Each individual certificate in the key store is also AES-GCM-256 encrypted individually using the DEK created during installation
6) The enrolled device certificate private keys are generated on the mobile device and signed by the intermediate CA on the applicable UEM server.
7) Additional trusted root CAs can be loaded to support accepting certificates from other devices (syslog, ldap, etc.).

1.5.4.3 Identification and authentication

The BlackBerry UEM server requires staff members to login prior to performing any security functions or accessing any services. Similarly, mobile devices must authenticate with the server using LDAP credentials prior to enrolling.

The BlackBerry UEM server uses X.509 certificates in conjunction with TLS to both authenticate and secure remote connections.

1.5.4.4 Security management

The BlackBerry UEM server facilitates granular administrative access to functions based on roles: server primary administrators, security administrators, administrators, managers, auditors, and mobile device users. Administrative users access the BlackBerry UEM server via a web-based interface. The BlackBerry UEM server also supports the definition of mobile device users, and upon enrolment each mobile device generates an X.509 certificate used to identify that enrolled device.

The BlackBerry UEM server provides all the features necessary to manage mobile device policies sent to enrolled mobile devices (via their device agents).

1.5.4.5 Protection of the TSF

The BlackBerry UEM server (TOE) and device agent (Non-TOE) work together to ensure that all security related communication between those components is protected from disclosure and modification.

1.5.4.6 Trusted path/channels

The BlackBerry UEM server uses TLS/HTTPS to secure communication channels between itself and remote staff agents accessing the server via a web-based user interface. It also uses TLS to secure communication channels between itself, enrolled devices, its configured SQL database server, syslog servers, and configured LDAP servers.

The following is a summary of applicable secure channels:

1) UEM server console and web services APIs used by staff members – TLS not subject to mutual X.509 authentication. Certicom implementation of TLS on server.
2) Mobile device agent to UEM server – TLS not subject to mutual X.509 authentication for initial enrollment, but always uses mutual X.509 authentication (with certificate pinning for iOS) once enrolled. Certicom implementation of TLS on server.
3) UEM server to SYSLOG and LDAP – TLS configured for mutual X.509 authentication in the evaluated configuration. Certicom implementation of TLS on server.

4) UEM server to SQL database – Communication with the SQL database is either local within the windows platform on which the UEM server executes or protected by IPSec provided by the windows platform and TLS.

1.5.5 TOE Environment

The TOE is installed on a Windows Server 2019 or Windows Server 2022 platform. For more information, see the UEM compatibility matrix. For the purposes of the evaluation, it is recommended to run UEM in a virtual environment (VMWare ESXi 8.0.2) on an AMD EPYC 7702P 64-Core Processor.

Ensure that database latency requirements are met. BlackBerry UEM Core servers must have less than 5ms latency to the database server.

The IT environment must also provide the following:

- a Microsoft SQL database server for managing the SQL database used by the UEM server (communication not protected in case of a local database server, communication protected by TLS and IPsec in case of a non-local database server)
- an IPsec channel implemented in the host Windows Server 2019/Windows Server 2022 operating system for all communication between the UEM Server and its non-local SQL database server.
- an NTP Server as a reliable time source
- LDAP for authentication of mobile device users and administrative users (communication protected by LDAPS/TLS)
- an optional SYSLOG server for external log storage (communication protected by TLS)
- optional Device Enrolment services for iOS and Android mobile devices including Apple DEP for iOS and KME for Android Samsung devices (communication protected by HTTPS/TLS)
- a push notification service for sending push notifications to mobile devices (communication protected by TLS)
- iOS and Android mobile devices and respective device agents (iOS device agent developed by Apple, BlackBerry UEM Android client) (communication protected by HTTPS/TLS)

Note: The security of the TOE is also dependent on its environment. All software and hardware platforms must be under support of their vendors, i.e. the operating system must get regular security updates and is not EOL.

1.5.6 Delivery and update

The BlackBerry UEM Server is delivered as an executable installer. It can be downloaded by customers from the BlackBerry customer portal https://support.blackberry.com/community/s/downloads.

The BlackBerry UEM server includes secure update capabilities to ensure the integrity of any updates so that updates will not introduce malicious or other unexpected changes in the TOE. Updates for the UEM server are distributed in a zip file. Unzipping results in an extractor exe file, data files, a manifest file, signature file, and 3rd party tools. The extractor is a signed executable (using a BlackBerry X.509 public certificate) and the signature is checked by the Windows Server

platform. The extractor file is then responsible for checking the signature file, which validates the manifest file and the signatures of the reminder of included files.

2 CONFORMANCE CLAIMS

2.1 CC conformance claim

This ST is CC Part 2 extended and CC Part 3 conformant and claims conformance to CC edition CC:2022 Revision 1.

The ST claims strict conformance to the PP-Configuration Mobile Device Management – Trusted Server (MDM-TS) [MDMTSPP] complemented with PP-Module Trusted Communication Channel (TCC), BSI-CC-PP-0116 [MDMTSPPC].

This ST claims conformance to the EAL 4 package of security assurance requirements, augmented with ALC_FLR.3.

2.2 Conformance rationale

The TOE type of this ST is the trusted server of an MDM system. This is the same TOE type as in the claimed PP-Configuration [MDMTSPPC].

This ST claims strict conformance with the components [MDMTSPP] and [TCCPPM] of the PP-Configuration [MDMTSPPC]. The security problem definition, security objectives and security requirements defined in this ST are consistent with those defined by the components of the PP-Configuration based on the following rationale:

- The security problem definition and the security objectives are all taken from [MDMTSPP] and [TCCPPM]. No other threats, organisational security policies and assumptions have been added in this ST. As the TOE provides a trusted communication channel, OT.TRUSTEDCOMMUNICATIONCHANNEL as defined in [TCCPPM] has been added to this ST and OE.TRUSTEDCOMMUNICATIONCHANNEL as defined in [MDMTSPP] has been removed.
- The security functional requirements (SFRs) specified in this ST include all SFRs specified in [MDMTSPP] and [TCCPPM]. The SFRs have been updated to conform to [CC:2022]. This does not violate strict conformance for the following reasons:
  - Most of the changes are minor editorial changes that do not modify the meaning of the SFRs.
  - FAU_STG.3 is now covered by FAU_STG.4 and its dependency has changed from FAU_STG.1 to FAU_STG.2; these changes only affect the numbering of the SFRs and not their meaning.
  - FCS_CKM.5 now depends on FCS_CKM.6 instead of FCS_CKM.4. FCS_CKM.4 is deprecated in [CC:2022]; its statements are included in FCS_CKM.6.
  - The dependencies of FCS_COP.1 have changed in [CC:2022]. This has been taken into account in this ST.
- The security assurance requirements (SARs) have been adopted from [MDMTSPP] without any changes. [TCCPPM] does not specify any SARs. No additional SARs have been added in this ST.

3 SECURITY PROBLEM DEFINITION

The security problem definition defines the security problem that is addressed by the TOE as well as the assumptions on the operational environment that are necessary for the TOE to be able to address the security problem.

The MDM Trusted Server interacts with two kinds of remote users:

- Device agents representing the managed mobile devices.
- Staff agents in three different roles: administrator agents, auditor agents, and manager agents. Each staff agent is associated with one or more roles.

According to the usage of the MDM Trusted Server, four types of threat agents are considered:

- Malicious device agent – an external entity interacting with the mobile device interface of the MDM device server component.
- Malicious staff agent – an external entity interacting with the staff interface of the MDM control server component.
- Malicious MDM proxy – an external entity acting as a proxy of any staff agent, any device agent, or the MDM device/control server component.
- Network attacker – a threat agent attempting to compromise network communication between external entities and the MDM device/control server component.

The assets consist of the user data that is stored, received, and transmitted by the TOE.

3.1 Threats

This section of the security problem definition describes the threats that are countered by the TOE, its operational environment, or a combination of the two. The threats have been taken from [MDMTSPP] and [TCCPPM].[2]

Threat agents are typically characterized by a number of factors such as expertise, available resources, and motivation, with the motivation being linked directly to the value of the assets at stake.

Threat	Description
T.MALICIOUSDEVICE	A malicious device agent may gain unauthorised logical access to the MDM device server component in order to cause unauthorised execution of management functions (in particular enrolment or unenrolment), to disclose or modify user data, or to compromise the MDM device server component.
T.MALICIOUSSTAFF	A malicious staff agent may gain unauthorised logical access to the MDM control server component in order to cause unauthorised execution of management functions, to disclose or modify user data, or to compromise the MDM control server component.
T.MASQUERADING	A malicious MDM proxy may masquerade as an authorised device agent, an authorised staff agent, or the MDM device/control server component in

[2] T.COMPROMISEDCOMMUNICATION is defined in [MDMTSPP] and [TCCPPM]. The other threats are defined in [MDMTSPP].

Threat	Description
	order to disclose or modify user data exchanged between the MDM device/control server component and authorised device/staff agents.
T.COMPROMISEDCOMMUNICATION	A network attacker may gain unauthorised logical access to communication channels in order to disclose or modify data exchanged between parts of the TOE and remote external entities.
T.COMPROMISEDSTORAGE	A malicious MDM proxy may gain unauthorised logical access to storage media in order to disclose or modify user data processed by the MDM device/control server component.

Table 1: Threats

3.2 Organisational security policies

The following organisational security policies (OSPs) are to be enforced by the TOE and the TOE environment. They have been taken from [MDMTSPP].[3]

OSP	Description
P.SEPARATION	The MDM Trusted Server shall separate interaction with authorised device agents from interaction with authorised staff agents. The MDM device server component shall communicate with device agents. The MDM control server component shall communicate with staff agents. The TOE shall prevent unauthorised disclosure or modification of data when it is transmitted between device agents, staff agents and MDM device/control server components.
P.MANAGEMENT	The MDM Trusted Server shall provide management of mobile devices by providing management functions as specified in Table 12. Management functions shall be performed only on behalf of authorised device/manager agents. The performance of management functions shall be controlled based on a hierarchical grouping relationship of authorised device/ manager agents.

Table 2: OSPs

3.3 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives. They have been taken from [MDMTSPP][4].

Assumption	Description
A.PROPERSTAFF	Staff members are assigned and authorised as administrator, auditor or manager based on their competence, skills, and training. They are trusted to not act in a careless, negligent, or hostile manner. They have access to operational user guidance and follow the instructions.

[3] [TCCPPM] does not define any organisational security policies.

[4] [TCCPPM] does not define any assumptions on the TOE environment.

Assumption	Description
A.PROPERUSER	Mobile device users are well informed about security measures and how to respond to security incidents. Mobile device users are assumed to immediately notify an authorised manager if a mobile device is lost or stolen so that the manager may apply remediation actions via the MDM Trusted Server.
A.PROPERMANAGEMENT	Mobile device management activities, including updates of applications and the operating system, are assumed to be performed cautiously, carefully and regularly. Authorised managers are in the performance of their tasks assumed to have due regard to the balance of stability and security of mobile device settings and configurations.
A.RESILIENCE	The operational environment provides sufficient security measures to ensure availability and resilience of the MDM Trusted Server.

Table 3: Assumptions

4 SECURITY OBJECTIVES

The security objectives provide a concise statement of the intended response to the security problem. It will describe which security need will be addressed by the TOE and which will be addressed by the TOE environment, in the form of a statement of security objectives.

4.1 Security objectives for the TOE

The following security objectives are to be met by the TOE. They have been taken from [MDMTSPP] and [TCCPPM].

Objective[5]	Description
OT.COMMUNICATION	The TOE shall prevent unauthorised disclosure and modification of data exchanged between parts of the TOE and remote authorised external entities by establishing and maintaining mutually authenticated trusted communication paths. The protection of confidentiality and integrity shall be based on the use of trusted communication channels.
OT.DEVICELIFECYCLE	The TOE shall protect the life-cycle of mobile devices by providing a trusted communication path between the TSF and each authorised device agent for device enrolment services, and by restricting the control over all device life-cycle management activities to authorised administrator agents.
OT.DEVICETRACKING	The TOE shall provide reliable logging facilities, that record all management activities of mobile devices including events concerning the life-cycle of mobile devices and any configuration changes of mobile devices. The logging facilities shall include the identities of the authorised device agents concerned. Review of the audit records shall be restricted to authorised auditor agents or authorised manager agents, and selectable with respect to the hierarchical grouping of device and staff agents.
OT.LOGGING	The TOE shall provide reliable logging facilities, that record all actions of authorised staff agents. The logging facilities shall include the identities of the authorised staff agents concerned. Review of the audit records shall be restricted to authorised auditor agents.
OT.MANAGEMENT	The TOE shall provide management of mobile devices by providing management functions as specified in Table 12. Management functions shall be performed only on behalf of authorised device agents or authorised manager agents. The

[5] OT.COMMUNICATION is defined in [MDMTSPP] and has been refined in [TCCPPM] to include trusted communication channels. OT.TRUSTEDCOMMUNICATIONCHANNEL is defined in [TCCPPM]. The remaining objectives are defined in [MDMTSPP].

Objective[5]	Description
	performance of management functions shall be controlled based on a hierarchical grouping relationship of authorised device agents and authorised manager agents.
OT.SEPARATION	The TOE shall separate interaction with authorised device agents from interaction with authorised staff agents. The MDM device server component shall communicate with device agents. The MDM control server component shall communicate with staff agents. The TOE shall prevent unauthorised disclosure or modification of data when it is transmitted between authorised device agents, authorised staff agents and MDM device/control server components.
OT.STORAGE	The TOE shall prevent unauthorised disclosure or modification of user data when it is stored on persistent storage media.
OT.TRUSTEDCOMMUNICATIONCHANNEL	The TOE shall provide mutually authenticated trusted communication channels. The TOE shall implement the trusted communication channels using trusted channel protocols based on cryptographic mechanisms.

Table 4: Security objectives for the TOE

4.2 Security objectives for the operational environment

The following security objectives, defined by [MDMTSPP] [6], are to be met by the TOE environment. As the TOE provides a trusted communication channel, OT.TRUSTEDCOMMUNICATIONCHANNEL as defined in [TCCPPM] has been added to this ST and OE.TRUSTEDCOMMUNICATIONCHANNEL as defined in [MDMTSPP] has been removed.

Objective	Description
OE.PROPERSTAFF	All authorised administrators, auditors and managers shall be competent, skilled and trained. They shall follow and apply TOE user guidance in a trusted manner.
OE.PROPERUSER	Mobile device user's awareness concerning security measures shall be assured. This includes the handling of security incidents as well as the acceptance of notifications. Mobile device users shall immediately notify an authorised manager if a mobile device is lost or stolen so that the manager may apply remediation actions via the TOE.
OE.PROPERMANAGEMENT	Mobile device management activities, including updates of applications and the operating system, shall be performed cautiously, carefully and

[6] [TCCPPM] does not define security objectives for the TOE environment.

Objective	Description
	regularly. Authorised managers shall in the performance of their tasks have due regard to the balance of stability and security of mobile device settings and configurations.
OE.RESILIENCE	The security configuration settings of the operational environment shall be appropriately adjusted to support availability and resilience of the TOE.
OE.DEVICELIFECYCLE	The device agents shall provide suitable technical means for trusted device enrolment, protected storage and communication, and execution of management functions during the mobile device life-cycle. Security measures and configuration settings of mobile devices shall be regularly checked and adjusted by authorised managers.
OE.SUPPORTINGSERVICES	The operational environment shall establish suitable technical means for the protection of all supporting services including their connection to the TOE. In particular, the operational environment shall provide a trusted enrolment service for mobile devices.
OE.RELIABLETIMESTAMPS	The operational environment shall provide reliable timestamps.
OE.AUDITTRAIL	The operational environment shall protect the stored audit records in the audit trail from unauthorised deletion or unauthorised modification.

Table 5: Security objectives for the operational environment

4.3 Security objectives rationale

All security objectives trace to threats and organisational security policies (see Table 6).

All security objectives for the operational environment trace to assumptions (see Table 7).

	T.MALICIOUSDEVICE	T.MALICIOUSSTAF	T.MASQUERADING	T.COMPROMISED-COMMUNICATION	T.COMPROMISED-STORAGE	P.SEPARATION	P.MANAGEMENT
OT.COMMUNICATION	x	x	x	x		x	
OT.DEVICELIFECYCLE	x	x					
OT.DEVICETRACKING	x						

	T.MALICIOUSDEVICE	T.MALICIOUSSTAF	T.MASQUERADING	T.COMPROMISED-COMMUNICATION	T.COMPROMISED-STORAGE	P.SEPARATION	P.MANAGEMENT
OT.LOGGING		x					
OT.MANAGEMENT	x	x					x
OT.SEPARATION	x	x	x			x	
OT.STORAGE					x		
OT.TRUSTEDCOMMUNICATIONCHANNEL	x	x	x	x		x	
OE.PROPERSTAFF	x	x					x
OE.PROPERUSER	x						x
OE.PROPERMANAGEMENT							x
OE.RESILIENCE							x
OE.DEVICELIFECYCLE	x						x
OE.SUPPORTINGSERVICES	x	x	x		x		x
OE.RELIABLETIMESTAMPS	x	x					
OE.AUDITTRAIL		x					

Table 6: Tracing of security objectives to threats and organisational security policies

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

The threat **T.MALICIOUSDEVICE** is countered by the objectives OT.COMMUNICATION, OT.SEPARATION, OT.MANAGEMENT, OT.DEVICELIFECYCLE, and OT.DEVICETRACKING which are supported by the objectives OE.PROPERSTAFF, OE.PROPERUSER, OE.DEVICELIFECYCLE, OE.SUPPORTINGSERVICES, OT.TRUSTEDCOMMUNICATIONCHANNEL, and OE.RELIABLETIMESTAMPS as these objectives ensure that unauthorised logical access of malicious device agents to the MDM device server component is prevented.

The threat **T.MALICIOUSSTAFF** is countered by the objectives OT.COMMUNICATION, OT.SEPARATION, OT.MANAGEMENT, OT.DEVICELIFECYCLE, and OT.LOGGING which are supported by the objectives OE.PROPERSTAFF, OE.SUPPORTINGSERVICES, OT.TRUSTEDCOMMUNICATIONCHANNEL, OE.RELIABLETIMESTAMPS and OE.AUDITTRAIL as these objectives ensure that unauthorised logical access of malicious staff agents to the MDM control server component is prevented.

The threat **T.MASQUERADING** is countered by the objectives OT.SEPARATION, and OT.COMMUNICATION which are supported by the objectives OE.SUPPORTINGSERVICES, and OT.TRUSTEDCOMMUNICATIONCHANNEL, as these objectives ensure the separation of communication paths and the protection of communication from disclosure and modification.

The threat **T.COMPROMISEDCOMMUNICATION** is countered by the objective OT.COMMUNICATION which is supported by the objective OT.TRUSTEDCOMMUNICATIONCHANNEL, as these objectives ensure the protection from unauthorised disclosure and modification of data exchanged between parts of the TOE and remote external entities by providing mutually authenticated trusted communication channels using trusted channel protocols based on cryptographic mechanisms.

The threat **T.COMPROMISEDSTORAGE** is countered by the objective OT.STORAGE which is supported by the objective OE.SUPPORTINGSERVICES for user data stored by the MDM device/control server component.

The organisational security policy **P.SEPARATION** is enforced by the objectives OT.SEPARATION, OT.COMMUNICATION and OT.TRUSTEDCOMMUNICATIONCHANNEL, as these objectives ensure the separation of interaction with authorised device agents from interaction with authorised staff agents.

The organisational security policy **P.MANAGEMENT** is enforced by the objective OT.MANAGEMENT which is supported by the objectives OE.PROPERSTAFF, OE.PROPERUSER, OE.PROPERMANAGEMENT, OE.RESILIENCE, OE.DEVICELIFECYCLE, and OE.SUPPORTINGSERVICES.

	A.PROPERSTAFF	A.PROPERUSER	A.PROPERMANAGEMENT	A.RESILIENCE
OE.PROPERSTAFF	x			
OE.PROPERUSER		x		
OE.PROPERMANAGEMENT			x	
OE.RESILIENCE				x
OE.DEVICELIFECYCLE				
OE.SUPPORTINGSERVICES				
OE.RELIABLETIMESTAMPS				
OE.AUDITTRAIL				

Table 7: Tracing of security objectives for the operational environment to assumptions

The assumption **A.PROPERSTAFF** is directly justified through the objective OE.PROPERSTAFF.

The assumption **A.PROPERUSER** is directly justified through the objective OE.PROPERUSER.

The assumption **A.PROPERMANAGEMENT** is directly justified through the objective OE.PROPERMANAGEMENT.

The assumption **A.RESILIENCE** is directly justified through the objective OE.RESILIENCE.

5 EXTENDED COMPONENTS DEFINITION

[MDMTSPP] and [TCCPPM] define several extended components. As most of them are now part of the [CC:2022] standard, it is no longer necessary to include them as extended components in this Security Target. Therefore, this Security Target only adopts the extended component FDP_ITT.1X defined in [MDMTSPP]

5.1 Internal TOE transfer (FDP_ITT)

Family behaviour

See CC Part 2, section 11.10.1

Components levelling and description

Figure 3 shows the component levelling for this family.

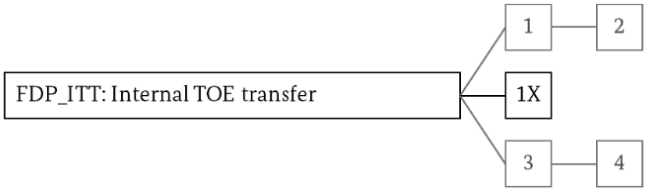

Figure 3: FDP_ITT: Component levelling

FDP_ITT.1X *Simple internal transfer protection*, requires that user data be protected when transmitted between parts of the TOE. It is a generalisation of FPD_ITT.1 *Basic internal transfer protection*.

The components FDP_ITT.1/.2/.3/.4 are already defined (see CC Part 2, section 11.10.2).

Management of FDP_ITT.1X

The following actions can be considered for the management functions in FMT:

a) If the TSF provides multiple methods to protect user data during transmission between separated parts of the TOE, the TSF can provide a pre-defined role with the ability to select the method that will be used.

Audit of FDP_ITT.1X

The following actions should be auditable if FAU_GEN *Security audit data generation* is included in the PP, PP-Module, functional package, or ST:

b) minimal: Successful transfers of user data, including identification of the protection method used.

c) basic: All attempts to transfer user data, including the protection method used and any errors that occurred.

FDP_ITT.1X Simple internal transfer protection

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.1X.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between separate parts of the TOE.

6 SECURITY REQUIREMENTS

6.1 Security functional requirements

This chapter describes the Security Functional Requirements (SFRs) for the TOE. The SFRs have been taken from [MDMTSPP] and [TCCPPM] and augmented by some additional SRFs in order to satisfy dependencies that have to be addressed by the ST author as stated in [TCCPPM].

The following table provides the list of SFR components claimed in this ST and the source document for each SFR.

SFR component	Source document
FAU_GEN.1	[MDMTSPP]
FAU_GEN.2	[MDMTSPP]
FAU_SAR.1	[MDMTSPP]
FAU_SAR.2	[MDMTSPP]
FAU_SAR.3	[MDMTSPP]
FAU_STG.4	[MDMTSPP]
FCS_CKM.1/ECDSA	added to satisfy dependencies
FCS_CKM.1/RSA	added to satisfy dependencies
FCS_CKM.2/ECDHE	added to satisfy dependencies
FCS_CKM.5	[TCCPPM]; several iterations (/SYMM, /MAC)
FCS_CKM.6	added to satisfy dependencies
FCS_COP.1	[TCCPPM]; several iterations (/AES ,/RSA, /ECDSA, /SHA, /HMAC)
FCS_RNG.1	[CC:2022], [AIS20]
FDP_IFC.1	[MDMTSPP]
FDP_IFF.2	[MDMTSPP]
FDP_ITT.1X	[MDMTSPP]
FDP_RIP.1	[MDMTSPP]
FDP_SDC.1	[MDMTSPP]
FDP_SDI.1	[MDMTSPP]
FDP_UCT.1	[MDMTSPP]
FDP_UIT.1	[MDMTSPP]
FIA_ATD.1	[MDMTSPP]
FIA_UAU.1/DA	[MDMTSPP]
FIA_UAU.1/SA	[MDMTSPP]
FIA_UID.1/DA	[MDMTSPP]
FIA_UID.1SA	[MDMTSPP]

SFR component	Source document
FIA_USB.1	[MDMTSPP]
FMT_MOF.1	[MDMTSPP]
FMT_MSA.1	[MDMTSPP]
FMT_MSA.3	[MDMTSPP]
FMT_SMF.1/AD	[MDMTSPP]
FMT_SMF.1/AU	[MDMTSPP]
FMT_SMF.1/MA	[MDMTSPP]
FMT_SMR.1	[MDMTSPP]
FPT_ITT.1	[MDMTSPP]
FTP_ITC.1	added to model additional services
FTP_PRO.1	[TCCPPM]
FTP_PRO.2	[TCCPPM]
FTP_PRO.3	[TCCPPM]
FTP_TRP.1/EN	[MDMTSPP]
FTP_TRP.1/DA	[MDMTSPP], inherited by [TCCPPM]
FTP_TRP.1/SA	[MDMTSPP], inherited by [TCCPPM]

Table 8: Source of SFR components

[MDMTSPP] and [TCCPPM] claim conformance to [CC3.1R5]. As this ST claims conformance to [CC:2022], the SFRs have been updated to conform to [CC:2022] where necessary. Minor editorial changes compared to [CC3.1R5] that do not modify the meaning have not been marked as changes in this ST. Other changes compared to [CC3.1R5] are marked with a corresponding footnote.

The following convention is used for operations applied to the SFRs by the ST author: Assignments and selections are indicated by **bold**. Refinements are indicated by **bold underscore** for additions and by ~~**bold strike through**~~ for deletions. Iterations are indicated by appending a slash and an identifier to the requirement, e.g. FCS_COP.1/AES.

Application notes adopted from [MDMTSPP] are labelled as “PP Application Notes”. Application notes adopted from [TCCPPM] are labelled as “PPM Application Notes”. ST application notes are simply noted as “ST Application Notes”.

This ST does not identify (i.e. highlight) assignments, selections and refinements already applied by the PP author.

6.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the basic level of audit **listed in Table 9**;

c) device enrolment, device unenrolment and **disablement/enablement of device workspace**; and

d) configuration changes of mobile devices regarding

i. installed certificates

ii. device settings

iii. operating system version / patch level

iv. installed applications incl. version

v. and **no other configuration changes of mobile devices**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, **no other audit relevant information**.

Requirement	**Auditable event**
FAU_GEN.1	None
FAU_GEN.2	None
FAU_SAR.1	Basic: Reading of information from the audit records
FAU_SAR.2	Basic: Unsuccessful attempts to read information from the audit records
FAU_SAR.3	None
FAU_STG.4	Basic: Actions taken due to exceeding of a threshold
FCS_CKM.1/ECDSA, /RSA	Minimal: Success and failure of the activity Basic: The object attribute(s), and object value(s) excluding any sensitive information
FCS_CKM.2	Minimal: Success and failure of the activity Basic: The object attribute(s), and object value(s) excluding any sensitive information
FCS_CKM.5	Minimal: Success and failure of the activity Basic: The object attribute(s), and object value(s) excluding any sensitive information
FCS_CKM.6	Minimal: Success and failure of the activity Basic: The object attribute(s), and object value(s) excluding any sensitive information
FCS_COP.1	Minimal: Success and failure, and the type of cryptographic operation Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes
FCS_RNG.1	None
FDP_IFC.1	None
FDP_IFF.2	Minimal: Decisions to permit requested information flows Basic: All decisions on requests for information flow
FDP_ITT.1X	Minimal: Successful transfers of user data, including identification of the protection method used

Requirement	Auditable event
	Basic: All attempts to transfer user data, including the protection method used and any errors that occurred
FDP_RIP.1	None
FDP_SDC.1	None
FDP_SDI.1	Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed
FDP_UCT.1	Minimal: The identity of any user or subject using the data exchange mechanisms Basic: The identity of any unauthorised user or subject attempting to use the data exchange mechanisms Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the information
FDP_UIT.1	Basic: The identity of any user or subject using the data exchange mechanisms. Basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so. Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data. Basic: Any identified attempts to block transmission of user data.
FIA_ATD.1	None
FIA_UAU.1	Minimal: Unsuccessful use of the authentication mechanism Basic: All use of the authentication mechanism
FIA_UID.1	Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided Basic: All use of the user identification mechanism, including the user identity provided
FIA_USB.1	Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject)
FMT_MOF.1	Basic: All modifications in the behaviour of the functions in the TSF
FMT_MSA.1	Basic: All modifications of the values of security attributes
FMT_MSA.3	Basic: Modifications of the default setting of permissive or restrictive rules Basic: All modifications of the initial values of security attributes
FMT_SMF.1	Minimal: Use of the management functions
FMT_SMR.1	Minimal: Modifications to the group of users that are part of a role
FPT_ITT.1	None
FTP_ITC.1	Minimal: Failure of the trusted channel functions. Minimal: Identification of the initiator and target of failed trusted channel functions.

Requirement	Auditable event
	Basic: All attempted uses of the trusted channel functions. Basic: Identification of the initiator and target of all trusted channel functions.
FTP_PRO.1	Minimal: Failure of the trusted channel establishment. Minimal: Identification of the initiator and target of failed trusted channel establishment. Basic: All attempted uses of the trusted channel. Basic: Identification of the initiator and target of all trusted channel attempts.
FTP_PRO.2	Minimal: Authentication failures during channel establishment. Basic: All authentication attempts.
FTP_PRO.3	Minimal: Failures when attempting to verify channel properties in FTP_PRO.3.2
FTP_TRP.1	Minimal: Failures of the trusted path functions. Minimal: Identification of the user associated with all trusted path failures, if available. Basic: All attempted uses of the trusted path functions. Basic: Identification of the user associated with all trusted path invocations, if available.

Table 9 MDM Server – Auditable events

PP Application Note (FAU_GEN.1). The ST author should list all types of audit records as required by FAU_GEN.1 in the TOE summary specification. If the TOE provides several audit levels, the ST author should indicate in the TOE summary specification how the minimum or basic level of audit of each auditable event is mapped to audit levels of the TOE.

6.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

PP Application Note (FAU_GEN.2). This PP considers device agents and staff agents as users. The ST author should describe in the TOE summary specification how auditable events are associated with the identity of device agents and staff agents.

6.1.3 FAU_SAR.1 Audit review

The following actions should be auditable (minimum or basic level of audit):

a) Basic: Reading of information from the audit records.

FAU_SAR.1.1 The TSF shall provide authorised staff agents as specified in Table 10, with the capability to read the list of audit information as specified in Table 10 from the audit data.

FAU_SAR.1.2 The TSF shall provide the audit data in a manner suitable for the staff agent to interpret the information.

Authorised users	List of audit information
auditor agents, i.e. staff agents associated with role auditor	all audit information

Authorised users	List of audit information
manager agents, i.e. staff agents associated with role manager	all audit information related to management activities of mobile devices including events concerning the life-cycle of mobile devices or any configuration changes of mobile devices

Table 10: Audit review capabilities

PP Application Note (FAU_SAR.1). This PP considers staff agents as external IT entities. The ST author should describe in the TOE summary specification how the audit information is unambiguously represented in an electronic fashion suitable for interpretation by staff agents.

6.1.4 FAU_SAR.2 Restricted audit review

The following actions should be auditable (minimum or basic level of audit):

a) Basic: Unsuccessful attempts to read information from the audit records.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

PP Application Note (FAU_SAR.2). According to FAU_SAR.1, auditor agents and manager agents have been granted explicit read access to the audit records. The ST author should describe in the TOE summary specification how read access of administrator agents and device agents is prohibited.

6.1.5 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply filtering of audit data based on the following criteria with logical relations for an arbitrarily chosen cluster of groupings, the staff agent reviewing the audit data, and the device agent associated with an audit record:

- each grouping of the chosen cluster is smaller than or equal to at least one grouping of the staff agent cluster of groupings; and
- the infimum of at least one grouping of the chosen cluster and the device agent grouping is not equal to the bottom grouping.

PP Application Note (FAU_SAR.3). The ability to apply filtering of audit data is expressed in terms of the bounded lattice of groupings as required by FDP_IFF.2.6. The staff agent reviewing the audit data chooses a cluster of groupings such that each grouping is upper-bounded by at least one grouping of its own cluster. All filtered audit records are associated with a device agent in such a way that the device agent grouping and at least one grouping of the chosen cluster have a common substantial lower bound, i.e. they meet at an infimum grouping greater than the bottom grouping. The ST author should describe in the TOE summary specification how the staff agent can choose a specific cluster of groupings and how the audit records are filtered according to the chosen cluster.

6.1.6 FAU_STG.4 Action in case of possible audit data loss[7]

The following actions should be auditable (minimum or basic level of audit):

a) Basic: Actions taken due to exceeding of a threshold.

[7] In [CC:2022], action in case of possible audit data loss is covered by FAU_STG.4 instead of FAU_STG.3 as in [CCV3.1R5]. Dependencies have changed from FAU_STG.1 to FAU_STG.2. This section has been updated to reflect these changes.

FAU_STG.4.1 The TSF shall **erase stored audit data** if the audit data storage exceeds **the lifetime for audit records of a value between 1 and 365 days configurable by the administrator**.

PP Application Note (FAU_STG.4). The action to be taken in case of a possible audit storage failure may require selecting a subset of all auditable events. In this case the PP/ST author should add FAU_SEL.1 to the security functional requirements.

ST Application Note (FAU_STG.4). FAU_STG.4.1 usually expects an action if the TOE detects that a certain amount or percentage of the available storage space for audit records has been exceeded. The audit data generated by the TOE is stored on the TOE's SQL database. The BlackBerry UEM Administrative Guidance Document defines SQL Server settings for the database that ensure that within the configurable lifetime of 1 to 365 days the audit storage cannot be exceeded.

6.1.7 FCS_CKM.1/ECDSA Cryptographic key generation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information.

FCS_CKM.1.1/ECDSA The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECC schemes** and specified **elliptic curves ~~cryptographic key sizes~~ NIST curves P-256, P-384, P-521, no other curves** that meet the following: **FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4**.

ST Application Note (FCS_CKM.1). FCS_CKM.1/ECDSA is used in support of ECDHE key establishment in TLS communication.

6.1.8 FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA schemes** and specified cryptographic key sizes **3072-bit or greater** that meet the following: **FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3**.

ST Application Note (FCS_CKM.1). FCS_CKM.1 is used for the generation of keys used for authentication in TLS communication.

6.1.9 FCS_CKM.2/ECDHE Cryptographic key distribution

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information.

FCS_CKM.2.1/ECDHE The TSF shall **~~distribute cryptographic keys~~ perform cryptographic key establishment** in accordance with a specified cryptographic key **~~distribution~~ establishment** method **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'**.

ST Application Note (FCS_CKM.2). FCS_CKM.2 is used for the ephemeral key establishment in TLS communication.

6.1.10 FCS_CKM.5/SYMM Cryptographic key derivation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information.

FCS_CKM.5.1/SYMM The TSF shall derive cryptographic keys **symmetric keys** from **master_secret, "key expansion", server_random + client_random** in accordance with a specified cryptographic key derivation algorithm **TLS KDF** and specified cryptographic key sizes **16, 32 bytes** that meet the following: **RFC 5246 section 6.3**.

PPM Application notes (FCS_CKM.5).

The PP/ST author shall iterate FCS_CKM.5 if necessary to cover all corresponding dependencies concerning cryptographic key derivation arising from FTP_PRO.2 or iterations thereof.

According to the dependencies of FCS_CKM.5, the PP/ST author shall further include the necessary FCS_CKM.2, FCS_COP.1 and/or FCS_CKM.4[8] components, to cover all corresponding cryptographic key derivation mechanisms as specified in FCS_CKM.5 or iterations thereof.

ST Application Note (FCS_CKM.5/SYMM). FCS_CKM.5/SYMM is used for the derivation of symmetric keys in TLS communication.

6.1.11 FCS_CKM.5/MAC Cryptographic key derivation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information.

FCS_CKM.5.1/MAC The TSF shall derive cryptographic keys **MAC keys** from **master_secret, "key expansion", server_random + client_random** in accordance with a specified cryptographic key derivation algorithm **TLS KDF** and specified cryptographic key sizes **32, 48 bytes** that meet the following: **RFC 5246 section 6.3**.

ST Application Note (FCS_CKM.5/MAC). FCS_CKM.5/MAC is used for the derivation of MAC keys in TLS communication.

6.1.12 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy all **plaintext keying material and critical security parameters (CSP)** when **no longer needed**.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **single direct overwrite consisting of zeroes** that meets the following: **none**.

ST Application Note (FCS_CKM.6). FCS_CKM.6 is used for the destruction of session keys that are generated in TLS communication.

6.1.13 FCS_COP.1/AES Cryptographic operation

The following actions should be auditable (minimum or basic level of audit):

[8] Dependencies in the PPM Application notes still refer to [CCV3.1R5].

a) Minimal: Success and failure, and the type of cryptographic operation.

b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

FCS_COP.1.1/AES The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **AES with operating modes** and cryptographic key sizes that meet the **standards as defined in the** following **table**:

AES operating mode	Cryptographic key sizes [bits]	Standards
CBC mode	128, 256	FIPS PUB 197 and NIST SP 800-38A
GCM mode	128, 256	NIST SP 800-38D

ST Application Note (FCS_COP.1/AES). FCS_COP.1/AES is used for encryption and decryption within TLS communication.

PPM Application Notes (FCS_COP.1).

There are several SFRs in this PP-Module, which model functionality making use of cryptographic operations. The author of this PP-Module cannot decide, how many different cryptographic operations (also in terms of cryptographic algorithm, key size, and applicable standard) would be necessary for a concrete TOE. Therefore, it is left open to the PP/ST author to iterate FCS_COP.1 in a way that all SFR dependencies requiring FCS_COP.1 are satisfied, and that also all cryptographic operations, which are needed to cover the security objectives of the TOE, are included in the final set of SFRs of the PP/ST.

Furthermore, as the dependencies concerning the key management related to the cryptographic operation modelled by FCS_COP.1, i.e. FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.4,[9]

- may be satisfied very differently for different concrete TOEs,
- may be satisfied very differently even for different keys of the same TOE,
- may be rightfully left unsatisfied with a corresponding rationale given, or
- may be satisfied by the very same iteration of FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and/or FCS_CKM.4 even for several iterations of FCS_COP.1,

none of these dependencies SFRs have been included in this PP–Module already. It is up to the PP/ST author to make sure that all those dependencies will be satisfied for all iterations of FCS_COP.1 as finally stated in the PP/ST. Satisfaction of dependencies has to be shown in the SFR dependency rationale in the PP/ST for all iterations of all SFRs independently anyway.

To still allow a somehow meaningful dependency rationale and security requirements rationale in this PP–Module, in the following the dependencies and security functional requirements needing instances/iterations of FSC_COP.1 in the PP/ST are listed:

- cryptographic operation needed for FTP_PRO.2 shared secret establishment,
- cryptographic operation needed for FTP_PRO.2 key derivation,
- cryptographic operations ‘encryption and decryption’ according to FTP_PRO.3,
- cryptographic operation ‘integrity protection’ according to FTP_PRO.3.

In each iteration of FCS_COP.1 in the PP/ST, in the assignment about the ‘list of cryptographic operations’ the PP/ST author should also identify the corresponding keys being used. This will allow

[9] Dependencies listed in the PPM Application Notes are based on [CCV3.1R5].

to easily map the FCS_COP.1 iterations to the related dependencies and security objectives, respectively.

Finally, for all iterations of FCS_COP.1 the choice of cryptographic algorithms and cryptographic key sizes should ensure the minimum security level of 100 bit for all cryptographic operations in their corresponding use case or protocol. The PP/ST author should follow the recommendations of the latest edition of the BSI Technical Guideline TR-02102[10] on cryptographic mechanisms when choosing cryptographic primitives, protocols, and parameters. Depending on the certification scheme, other recommendations for the choice of cryptographic mechanisms, such as the SOG-IS Agreed Cryptographic Mechanisms[11], may also be considered.

6.1.14 FCS_COP.1/RSA Cryptographic operation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure, and the type of cryptographic operation.

b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

FCS_COP.1.1/RSA The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm **RSA Digital Signature Algorithm** and cryptographic key sizes **3072 bit or greater** that meet the following: **FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5**

ST Application Note (FCS_COP.1/RSA). FCS_COP.1/RSA is used for the RSA signature generation and verification performed as part of the authentication within TLS communication.

6.1.15 FCS_COP.1/ECDSA Cryptographic operation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure, and the type of cryptographic operation.

b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes, and object attributes.

FCS_COP.1.1/ECDSA The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm **ECDSA schemes** and ~~**cryptographic key sizes**~~ **NIST curves P-384, P-256, P-521** that meet the following: **FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6**

ST Application Note (FCS_COP.1/ECDSA). FCS_COP.1/ECDSA is used for the ECDSA signature generation and verification performed as part of the authentication within TLS communication.

6.1.16 FCS_COP.1/SHA Cryptographic operation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure, and the type of cryptographic operation.

[10] German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), Technical Guideline TR-02102 – Cryptographic Mechanisms: https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/tr02102/tr02102_node.html

[11] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms: https://www.sogis.eu/uk/supporting_doc_en.html

b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

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

ST Application Note (FCS_COP.1/SHA). FCS_COP.1/SHA is used in TLS communication and random number generation.

6.1.17 FCS_COP.1/HMAC Cryptographic operation

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Success and failure, and the type of cryptographic operation.

b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

FCS_COP.1.1/HMAC The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA-256, HMAC-SHA-384** and cryptographic key sizes **256 and 384 bits and message digest sizes 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.'**

ST Application Note (FCS_COP.1/HMAC). FCS_COP.1/HMAC is used in TLS communication.

6.1.18 FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **deterministic** random number generator **conforming to NIST SP800-90A Hash_DRBG with SHA2-512 core** that implements:

(DRG.3.1) **If initialized with a random seed by an entropy source that accumulates entropy from a platform-based RBG with a minimum of 256 bits of entropy, the internal state of the RNG shall have a minimum entropy of 256 bits.**

(DRG.3.2) **The RNG provides forward secrecy.**

(DRG.3.3) **The RNG provides backward secrecy even if the current internal state is known.**

FCS_RNG.1.2 The TSF shall provide **random numbers** that meet:

(DRG.3.4) **The RNG, initialized with a random seed that is 256 bits in in size, generates output for which 2^{19} strings of bit length 128 are mutually different with probability $1-2^{-10}$.**

(DRG.3.5) **Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A and no additional test suites.**

6.1.19 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the MDM grouping SFP on the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 11.

Subjects	Information	Operations
manager attendant with security attribute: cluster of groupings	transmitted/received user data with security attribute: cluster of groupings	initiation of a mobile device management function as specified in Table 12
device attendant with security attribute: grouping	transmitted/received user data with security attribute: cluster of groupings	execution of a mobile device management function as specified in Table 12.

Table 11: List of subjects, information, and operations covered by the MDM grouping SFP

Mobile Device Management Functions **Payloads to be transferred to device agents**
1) Enforce/Prevent the installation/update/deinstallation of applications
2) Enable/Disable installed applications – including enterprise applications
3) Restrict the installation of applications based on trusted sources, or positive list of allowed applications, negative list of denied applications
4) Enforce the update of system software from trusted sources Prevent the update of system software from untrusted sources
5) Remote lock (transition to locked state)
6) Remote wipe of protected data
~~**7) Activate/Deactivate obligatory encryption of persistent memory**~~ [12]
8) Configure the way how sensitive information or data is displayed in unprotected states Note: This supports, for example, to hide e-mail contents, headers or metadata in notifications or in locked state
9) Configure password authentication policy settings: a) minimum password length b) minimum password complexity c) maximum password lifetime d) maximal number (at most 10) of consecutive unsuccessful password authentications e) ~~**time delay after a specified number of consecutive unsuccessful password authentications**~~[13]

[12] The storage of encryption keys into persistent memory is managed by Apple/Google design.

[13] On iOS devices, there is a time delay after six failed passcode attempts. This is an iOS native setting that cannot be configured via MDM payloads. On Android devices, there is a time delay after five failed passcode attempts. This is a Samsung Android native setting that cannot be configured via KSP policy.

Mobile Device Management Functions **Payloads to be transferred to device agents**
10) Configure biometric authentication policy settings
~~**11) Configure push message policy settings**~~
12) <u>Android =</u> Activate/Deactivate developer mode, e.g. Android Debug Bridge (ADB) [14]
13) Query software integrity attestation status incl. jailbreak / rooting detection [15]
14) Query the status of security-related configuration settings including at least a) installed certificates b) device settings c) operating system version / patch level d) installed applications incl. version
15) Enable/Disable users to/from configuring system level certificates, e.g., custom root certificates
16) Configure custom certificate provisioning (both enrolment and renewal) using Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST), or other suitable protocols
17) Configure network connections (DNS, gateways, DHCP, protection, etc.)
18) Configure VPN settings/policies Note: This supports, in particular, the configuration of a (permanent where necessary) VPN connection to the German Federal Networks (Netze des Bundes – NdB)
19) Enable/Disable network services/interfaces, e.g., tethering, VPN, WiFi, Bluetooth, NFC
20) Enable/Disable sharing services, e.g., Android Nearby Share, iOS AirDrop
21) <u>Android =</u> Enable/Disable location services [16]
22) Enable/Disable data exchange with other devices via specific interfaces, e.g., USB storage media
23) Enable/Disable data synchronisation with cloud services

Table 12: Mobile Device Management Functions

[14] ADB is only applicable for Android, and not iOS.

[15] Android= UEM Server initiates the attestation process by sending a Play Integrity attestation request to the UEM Client on the device. The UEM Client calls the Google Play Integrity API, requesting an assessment of the device's security and integrity. Google Play returns device integrity attestation verdict to the UEM Client (e.g device is jailbroken) The UEM Client forwards the attestation response payload back to the UEM Server. The UEM Server evaluates the verdict and applies compliance actions based on the integrity results. iOS= Apple MDA can perform attestation on four device identifiers - OS version, nonce, udid and serial number. It doesn't directly detect root detection as part of Jailbroken device.

[16] Controlling of location service is only available for Android and not for iOS

ST Application Note (FDP_IFC.1). Regarding 16.) SCEP is used to configure custom certificate provisioning, EST is not supported.

The UEM supports several parameters for managing devices. To allow for efficient modelling of parameters, only the following four parameters have been selected to be within the TOE scope: OS type (OS), the OS version (OSV), Device Model (DM) including the Manufacturer (M). All four parameters fall into the category of straightforward bounded sub-lattices of groupings as defined in section 7.2 of [MDMTSPP]. The combination of the four parameters matches the case of a systematic combination of bounded sub-lattices as defined in 7.5 of [MDMTSPP].

The TOE allows to combine the four parameters and vary them independently. But the resulting policy depends on whether the selected values for OS, OSV, DM and M fit. This will be discussed below in more detail.

The TOE supports the following straightforward bounded sub-lattices of groupings:

a.) OS types (OSs)

Let *OSTypes* be the set of all OS types:

OSTypes = {$OSType_1$, ...$OSType_n$}

Lattice elements: OSs = {OS|OS ⊆ *OSTypes*} (the set of all subsets of *OSTypes*)

Partial ordering: $\forall U, V \in OSs: U \leq V \equiv U \subseteq V$ (subset relation)

Join function: $\forall U, V \in OSs: U \sqcup V = U \cup V$ (set union)

Meet function: $\forall U, V \in OSs: U \sqcap V = U \cap V$ (set intersection)

b.) OS versions (OSVs)

Let *OSVersions* be the set of all OS versions used by the users:

OSVersions = {$OSVersion_1$, ...$OSVersion_n$}

Lattice elements: OSVs = {OSV|OSV ⊆ *OSVersions*} (the set of all subsets of *OSVersions*)

Partial ordering: $\forall U, V \in OSVs: U \leq V \equiv U \subseteq V$ (subset relation)

Join function: $\forall U, V \in OSVs: U \sqcup V = U \cup V$ (set union)

Meet function: $\forall U, V \in OSVs: U \sqcap V = U \cap V$ (set intersection)

c.) DeviceModels (DMs)

Let *DeviceModels* be the set of all user groups defined in all associated LDAPs:

DeviceModels = {$DeviceModel_1$, ...$DeviceModel_n$}

Lattice elements: DMs = {DM|DM ⊆ *DeviceModels*} (the set of all subsets of *DeviceModels*)

Partial ordering: $\forall U, V \in DMs: U \leq V \equiv U \subseteq V$ (subset relation)

Join function: $\forall U, V \in DMs: U \sqcup V = U \cup V$ (set union)

Meet function: $\forall U, V \in DMs: U \sqcap V = U \cap V$ (set intersection)

d.) Manufacturers (Ms)

Let *Manufacturers* be the set of all Manufacturers:

Manufacturers = {$Manufacturer_1$, ...$Manufacturer_n$}

Lattice elements: Ms = {M|M ⊆ *Manufacturers*} (the set of all subsets of *Manufacturers*)

Partial ordering: $\forall U, V \in Ms: U \leq V \equiv U \subseteq V$ (subset relation)

Join function: $\forall U, V \in Ms: U \sqcup V = U \cup V$ (set union)

Meet function: $\forall U, V \in Ms: U \sqcap V = U \cap V$ (set intersection)

Combined lattice

The four sub-lattices defined above can be systematically combined into one bounded lattice. The elements of this latter reflect the possible groupings relevant for the MDM grouping SFP.

For the bounded sub-lattices on the set OSs of operating system groupings, the set of OSVs of operating system version groupings, the set of DM of device model groupings and the set of Ms of manufacturer groupings, all as defined above, we define the combined groupings and by this the combined bounded lattice component-by-component on ordered tuples:

Lattice elements: {(OS, OSV, DM, M) | OS ∈ OSs, OSV ∈ $OSVs$, DM ∈ DMs, M ∈ Ms}

Partial ordering: $(OS_1, OSV_1, DM_1, M_1) \leq (OS_2, OSV_2, DM_2, M_2) \equiv OS_1 \leq OS_2 \wedge OSV_1 \leq OSV_2 \wedge DM_1 \leq DM_2 \wedge M_1 \leq M_2$

Join function: $(OS_1, OSV_1, DM_1, M_1) \sqcup (OS_2, OSV_2, DM_2, M_2) = (OS_1 \sqcup OS_2, OSV_1 \sqcup OSV_2, DM_1 \sqcup DM_2, M_1 \sqcup M_2)$

Meet function: $(OS_1, OSV_1, DM_1, M_1) \sqcap (OS_2, OSV_2, DM_2, M_2) = (OS_1 \sqcap OS_2, OSV_1 \sqcap OSV_2, DM_1 \sqcap DM_2, M_1 \sqcap M_2)$

For a device attendant only one grouping at a time is supported. For a manager attendant a cluster of groupings (i.e. a combination of more than one grouping) is supported. If more than one grouping is assigned to the manager attendant, the effective grouping is the result of joining the single groupings using the join function for the combined lattice as defined above.

To determine the effective policy based on a grouping, the TOE allows to define 'ALL' and 'ANY' for the combination of the single groupings, where 'ALL' mandates that all parameters must match and 'ANY' requires that at least one of the parameters matches.

Refinement for items 9e.), 11.), 7.), 12.), 13.), 21.) of [MDMTSPP]

Table 5 in [MDMTSPP] defines 9e.) Configure password authentication policy settings: time delay after a specified number of consecutive unsuccessful password authentications. On iOS devices, there is a time delay after six failed passcode attempts. This is an iOS native setting that cannot be configured via MDM payloads. As the TOE does not allow the manager attendant to configure this time delay through the MDM, this item has been removed by formatting it in strikethrough. In the sense of the lattice model the modelling for payload for configuring password authentication policy settings in general does not change as only the group members for the time delay are missing in the lattice.

Table 5 in [MDMTSPP] defines 11.) Configure push message policy settings. The settings for how the UEM Server communicate with the APNS is hard coded to UEM and not configurable. As the TOE does not allow the manager attendant to configure these policy settings through the MDM, this item has been removed by formatting it in strikethrough. In the sense of the lattice model this corresponds to a fixed grouping of (OS, OSV, DM, M) = (∅, ∅, ∅, ∅).

Table 5 in [MDMTSPP] defines 7) The functions is not provided by the platforms and hence cannot be invoked by the UEM and for the iOS functionality, iOS does not provide the corresponding interactions, hence, they cannot be invoked by the UEM.

Table 5 in [MDMTSPP] defines 12) Currently there is no MDM developer mode IT Policy in UEM.

Table 5 in [MDMTSPP] defines 13) BlackBerry UEM uses Apple manage device attestation feature for any device attestation failure.

Table 5 in [MDMTSPP] defines 21) Apple does not provide MDM location service policy, for Android this can be done through KSP policy.

PP Application Note (MDM functions). The MDM functions specified in Table 12 may be modified by the PP/ST author in accordance with the restrictions for refinement operations. For instance, the TOE may be able to support profile templates for specific user subgroups. The configuration of such profile templates may be listed as an additional MDM function.

6.1.20 FDP_IFF.2 Hierarchical security attributes

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Decisions to permit requested information flows.

b) Basic: All decisions on requests for information flow.

FDP_IFF.2.1 The TSF shall enforce the MDM grouping SFP based on the following types of subject and information security attributes: the list of subjects and information, and for each, the security attributes as defined in Table 11.

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes, hold: for an arbitrarily chosen cluster of groupings of controlled information

- the initiation of a mobile device management function is permitted, if and only if each grouping of the chosen cluster is smaller than or equal to at least one grouping of the manager attendant cluster of groupings;
- the execution of a mobile device management function is permitted, if and only if the infimum of at least one grouping of the chosen cluster and the device attendant grouping is not equal to the bottom grouping.

FDP_IFF.2.3 The TSF shall enforce the following additional rules:

- distinct communication paths are used for information flows between manager attendant and manager agent on initiation of a mobile device management function and between device attendant and device agent on execution of a mobile device management function;
- the initiation and/or execution of a mobile device management function involves an information flow between manager attendant and device attendant ensuring that the cluster of groupings of controlled information remains unaltered;
- the execution of a mobile device management function involves the over-the-air transfer of the payload to the mobile device.

FDP_IFF.2.4 The TSF shall explicitly authorise an information flow based on the following rules: none.

FDP_IFF.2.5 The TSF shall explicitly deny an information flow based on the following rules: the execution of a mobile device management function is denied when the respective device is unable to perform the device command or to enforce the device policy.

FDP_IFF.2.6 The TSF shall enforce the following relationships for any two valid groupings:

a) there exists a partial ordering relation with a unique minimum (bottom grouping) and a unique maximum (top grouping) that, given two valid groupings, determines
if the groupings are equal, if one grouping is greater or lower than the other, or if the groupings are incomparable;

b) there exists a join function in the set of groupings, such that,
given any two valid groupings, there is a valid unique join grouping that is the supremum (least upper bound) of the two valid groupings;

c) there exists a meet function in the set of groupings, such that,
given any two valid groupings, there is a valid unique meet grouping that is the infimum (greatest lower bound) of the two valid groupings.

PP Application Note (MDM grouping SFP). The components FDP_IFC.1 and FDP_IFF.2 define rules for the relationship between manager attendants and device attendants by restricting the initiation and execution of MDM functions based on groupings that are associated with subjects and information. FDP_IFC.1 defines the name of the information flow control policy (MDM grouping SFP) and its scope of control. FDP_IFF.2 specifies the details of the information control policy. The TOE usually provides further restrictions on the initiation and execution of MDM functions, that may particularly be based on arbitrary selections of mobile devices. While any such further restrictions are not considered as part of the TOE security functionality, the ST author should describe in the TOE summary specification how the initiation and execution of MDM functions is controlled based on groupings as defined in this PP.

PP Application Notes (bounded lattice of groupings).

The rules of the MDM grouping SFP are based on the partial ordering relationship of groupings that is an essential part of the definition of a lattice of groupings (see PP appendix section 7 for some examples). It is important that the set of groupings is a lower-bounded lattice with bottom grouping, since otherwise the rules of the MDM grouping SFP were ill-defined. It is also important that the set of groupings is an upper-bounded lattice with top grouping, since this enables the existence of a management attendant associated with the top grouping, i.e. a top management attendant being able to manage all mobile devices.

The bounded lattice of groupings may be realised in various ways. For multi-tenancy support, the groupings may be expressed as sets of tenants with basic operations from set theory (see PP appendix section 7.2). Extended kinds of groupings may be constructed as tuples of groupings where the components of a tuple are combining e.g. a set of tenants with the elements of some other bounded lattices of groupings. The bottom and top elements, the partial ordering relation, and the join and meet functions of such tuples of groupings are defined component-by-component (see PP appendix section 7.5).

The ST author should describe in the TOE summary specification how the bounded lattice of groupings is realised. The description should include the definition of the bottom and top elements, the partial ordering relation, and the join and meet functions.

6.1.21 FDP_ITT.1X Simple internal transfer protection

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Successful transfers of user data,
including identification of the protection method used.

b) Basic: All attempts to transfer user data,
including the protection method used and any errors that occurred.

FDP_ITT.1X.1 The TSF shall enforce the MDM grouping SFP to prevent the disclosure and modification of user data when it is transmitted between device attendants and manager attendants.

PP Application Note (FDP_ITT.1X). Protection of user data is required while it is in transit between controlled subjects (active entities), i.e. device attendants and manager attendants, of the MDM grouping SFP (cf. FDP_IFC.1). The degree of separation of the controlled subjects depends on the architecture and design of the TOE. When device attendants and manager attendants are placed in physically or virtually separated parts of the TOE, e.g. TOE device server component and TOE control server component, the internal transfer of user data is performed using network communication. In other cases, the internal transfer may be performed using e.g. inter-container communication, shared services, etc. The ST author should describe in the TOE summary specification how the user data is protected from disclosure and modification while in transit within the TOE.

6.1.22 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: any buffer object that is used during the initiation or execution of a mobile device management function according to the MDM grouping SFP.

- **Plaintext PINs and passwords sent to the TOE for user authentication and reference values retrieved from the database are erased from the database storage after the user is deleted, or before it is updated;**
- **Ephemeral keys for TLS sessions are erased from volatile memory upon session termination**.

PP Application Note (FDP_RIP.1). Residual information, in particular special categories of user data such as PINs, passwords, cryptographic keys/certificates, etc., needs protection against re-use. The ST author should describe in the TOE summary specification how such residual information (i.e. previous information content) is made unavailable.

ST Application Note (FDP_RIP.1). The residual information that needs to be protected from unauthorized re-use in the context of the MDM grouping SFP are PINs and passwords entered by users for authentication to the TOE as well as ephemeral keys for TLS sessions.

6.1.23 FDP_SDC.1 Stored data confidentiality

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the following user data: special categories of user data, while it is stored in the persistent memory controlled by the TSF.

PP Application Note (FDP_SDC.1). Typical special categories of user data are PINs, passwords, cryptographic keys/certificates, etc. Various protection mechanisms may be used to ensure confidentiality. The ST author should describe in the TOE summary specification the protection mechanisms that are used by the TSF.

6.1.24 FDP_SDI.1 Stored data integrity monitoring

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check.

b) Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed.

FDP_SDI.1.1 The TSF shall monitor special categories of user data stored **encrypted** in persistent memory controlled by the TSF for **integrity errors during decryption** on all objects, based on the following attributes: **user passwords, PINs, passwords used for key derivation, X509v3 certificates and related private keys**.

PP Application Note (FDP_SDI.1). Typical special categories of user data are PINs, passwords, cryptographic keys/certificates, etc. Various protection mechanisms may be used to monitor integrity. The ST author should describe in the TOE summary specification the protection mechanisms that are used by the TSF.

6.1.25 FDP_UCT.1 Basic data exchange confidentiality

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: The identity of any user or subject using the data exchange mechanisms.

b) Basic: The identity of any unauthorised user or subject attempting to use the data exchange mechanisms.

c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the information.

FDP_UCT.1.1 The TSF shall enforce the MDM grouping SFP to transmit and receive user data in a manner protected from unauthorised disclosure.

6.1.26 FDP_UIT.1 Data exchange integrity

The following actions should be auditable (minimum or basic level of audit):

a) Basic: The identity of any user or subject using the data exchange mechanisms.

b) Basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so.

c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.

d) Basic: Any identified attempts to block transmission of user data.

FDP_UIT.1.1 The TSF shall enforce the MDM grouping SFP to transmit and receive user data in a manner protected from modification errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification has occurred.

6.1.27 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- staff agent security attributes: role, cluster of groupings;
- device agent security attributes: grouping.

6.1.28 FIA_UAU.1/DA Timing of authentication [iteration for device agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Unsuccessful use of the authentication mechanism.

b) Basic: All use of the authentication mechanism.

FIA_UAU.1.1/DA The TOE device server security functionality shall allow **no TSF mediated actions** on behalf of the device agent to be performed before the device agent is authenticated.

FIA_UAU.1.2/DA The TOE device server security functionality shall require each device agent to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that device agent.

6.1.29 FIA_UAU.1/SA Timing of authentication [iteration for staff agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Unsuccessful use of the authentication mechanism.

b) Basic: All use of the authentication mechanism.

FIA_UAU.1.1/SA The TOE control server security functionality shall allow **to request password recover, choose a language and select the authentication provider** on behalf of the staff agent to be performed before the staff agent is authenticated.

FIA_UAU.1.2/SA The TOE control server security functionality shall require each staff agent to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that staff agent.

6.1.30 FIA_UID.1/DA Timing of identification [iteration for device agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided.

b) Basic: All use of the user identification mechanism, including the user identity provided.

FIA_UID.1.1/DA The TOE device server security functionality shall allow **no TSF mediated actions** on behalf of the device agent to be performed before the device agent is identified.

FIA_UID.1.2/DA The TOE device server security functionality shall require each device agent to be successfully identified before allowing any other TSF-mediated actions on behalf of that device agent.

6.1.31 FIA_UID.1/SA Timing of identification [iteration for staff agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided.

b) Basic: All use of the user identification mechanism, including the user identity provided.

FIA_UID.1.1/SA The TOE control server security functionality shall allow **to request password recover, choose a language and select the authentication provider** on behalf of the staff agent to be performed before the staff agent is identified.

FIA_UID.1.2/SA The TOE control server security functionality shall require each staff agent to be successfully identified before allowing any other TSF-mediated actions on behalf of that staff agent.

6.1.32 FIA_USB.1 User-subject binding

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).

b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- staff agent security attributes: role, cluster of groupings;
- device agent security attributes: grouping.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- a staff attendant, i.e. a subject in the TOE control server acting on behalf of a staff agent, inherits the role and the cluster of groupings from that staff agent;
- a device attendant, i.e. a subject in the TOE device server acting on behalf of a device agent, inherits the grouping from that device agent.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **The TSF cannot modify user data maintained by LDAP (in case LDAP-based authentication is used), but only update user data by synchronizing data with LDAP. Managers can modify user data maintained by the MDM-TS directly on the TOE**.

ST Application Note (FIA_USB.1).

The TOE supports the creation of local users, but also allows to use users maintained in an LDAP server. In the latter case, the TOE handles user data that is synchronized with LDAP. This user data cannot be directly modified on the TOE, but only updated by modifying the data on LDAP and synchronizing with LDAP afterwards.

There is additional user data that is not maintained by LDAP and that can directly be modified on the TOE. Roles with permissions are maintained in the MDM-TS directly and not in LDAP.

All changes to the user data are audited.

6.1.33 FMT_MOF.1 Management of security functions behaviour

The following actions should be auditable (minimum or basic level of audit):

a) Basic: All modifications in the behaviour of the functions in the TSF.

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, and modify the behaviour of the device life-cycle management to the administrator role.

6.1.34 FMT_MSA.1 Management of security attributes

The following actions should be auditable (minimum or basic level of audit):

a) Basic: All modifications of the values of security attributes.

FMT_MSA.1.1 The TSF shall enforce the MDM grouping SFP to restrict the ability to change_default, query, modify or delete the information security attributes cluster of groupings to the manager role.

6.1.35 FMT_MSA.3 Static attribute initialisation

The following actions should be auditable (minimum or basic level of audit):

a) Basic: Modifications of the default setting of permissive or restrictive rules.

b) Basic: All modifications of the initial values of security attributes.

FMT_MSA.3.1 The TSF shall enforce the MDM grouping SFP to provide ~~**permissive**~~ **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall **not** allow the manager **or any other** role to specify alternative initial values to override the default values when information is created.

ST Application Note (FMT_MSA.3).

Refinement FMT_MSA.3.1: All permissions have to be actively assigned to a role. There is no set of default permissions. Thus, the default-like set of permission is 'no permissions'. This is a restrictive default value. Therefore, the SFR has been refined from 'permissive' to 'restrictive'. As 'restrictive' is stricter than 'permissive', this refinement should be acceptable.

Refinement FMT_MSA.3.2: The default list of permissions is empty and each permission needs to be explicitly granted for a role. This behaviour cannot be changed and no default set of permissions can be specified. While it is understandable for the original selection in FMT_MSA.3.1 to mandate that the manager can specify alternative initial values to create more strict TOE configurations, with the refinement for FMT_MSA.3.1 the TOE is already in its most secure configuration. Allowing the manager to specify alternative initial values (i.e. default permissions), the TOE configuration will not become more strict and potentially weaker. Therefore, FMA_MSA.3.2 has been refined to not to allow the manager or any other role to specify alternative initial values. As the refined definition for FMT_MSA.3.2 is stricter than the original definition for FMT_MSA.3.2 (in particular in the light of the refinement for FMT_MSA.3.1), this refinement should be acceptable.

6.1.36 FMT_SMF.1/AD Specification of Management Functions [iteration for administrator agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Use of the management functions.

FMT_SMF.1.1/AD The TSF shall be capable of performing the following management functions on behalf of a staff agent that is associated with the administrator role:

- determine the behaviour of, disable, enable, or modify the behaviour of the device life-cycle management including
  - device enrolment,
  - device unenrolment,
  - provisioning of credentials for identification/authentication of device agents, and
  - setting of device agent security attributes.

PP Application Note (FMT_SMF.1/AD – device life-cycle management). The device life-cycle management may include various activities. Processes for device (un-)enrolment and device agent

registration (provisioning of credentials, setting of security attributes) are not in the scope of this PP. If the TSF provides security features for device (un-)enrolment or device agent registration, the PP/ST author may add further management functions, and, as appropriate, other security functional requirements.

PP Application Note (FMT_SMF.1/AD – staff agent management). The staff agent management is not in the scope of this PP. If the TSF provides secure management of staff agents, the PP/ST author may add further management functions, and, as appropriate, other security functional requirements.

6.1.37 FMT_SMF.1/AU Specification of Management Functions [iteration for auditor agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Use of the management functions.

FMT_SMF.1.1/AU The TSF shall be capable of performing the following management functions on behalf of a staff agent that is associated with the auditor role:

- review audit information.

PP Application Note (FMT_SMF.1/AU – management of the audit function). The management of the audit function is not in the scope of this PP. If the TSF provides secure management of the audit function, the PP/ST author may add further management functions, a further iteration of FMT_MOF.1, and, as appropriate, other security functional requirements.

6.1.38 FMT_SMF.1/MA Specification of Management Functions [iteration for manager agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Use of the management functions.

FMT_SMF.1.1/MA The TSF shall be capable of performing the following management functions on behalf of a staff agent that is associated with the manager role:

- review audit information;
- change_default, query, modify or delete the information security attributes of the MDM grouping SFP.

6.1.39 FMT_SMR.1 Security roles

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Modifications to the group of users that are part of a role.

FMT_SMR.1.1 The TSF shall maintain the roles administrator, auditor, and manager.

FMT_SMR.1.2 The TSF shall associate staff agents with roles.

6.1.40 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

PP Application Note (FPT_ITT.1). Protection of TSF data is required while it is in transit between separate parts of the TSF in the TOE device server and the TOE control server. The degree of separation depends on the architecture and design of the TOE. The internal transfer of TSF data

may be performed using network communication or using e.g. inter-container communication, shared services, etc. The ST author should describe in the TOE summary specification how the TSF data is protected from disclosure and modification while in transit within the TOE.

6.1.41 FTP_ITC.1 Inter-TSF trusted channel

The following actions should be auditable (minimum or basic level of audit):

a) minimal: Failure of the trusted channel functions;

b) minimal: Identification of the initiator and target of failed trusted channel functions;

c) basic: All attempted uses of the trusted channel functions;

d) basic: Identification of the initiator and target of all trusted channel functions.

FTP_ITC.1.1 The TSF shall provide a communication channel **using TLS as defined in FTP_PRO.1** between itself and ~~**another trusted IT product**~~ **an LDAP server, an external audit server, a remote database server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- **exporting audit records to an external audit server**
- **authentication through the LDAP server**
- **accessing the MDM Server's SQL database in case of a remote database server**

6.1.42 FTP_PRO.1 Trusted channel protocol

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Failure of the trusted channel establishment.

b) Minimal: Identification of the initiator and target of failed trusted channel establishment.

c) Basic: All attempted uses of the trusted channel.

d) Basic: Identification of the initiator and target of all trusted channel attempts.

Other events should be considered according to the specific protocols used.

FTP_PRO.1.1 The TSF shall implement **TLS v1.2 and no earlier TLS versions** acting as **a client, a server** in accordance with: **RFC 5246**.

FTP_PRO.1.2 The TSF shall enforce usage of the trusted channel **for the following purposes**:

When acting as a TLS server:

- **protecting communication channels between the MDM Server and device agent**
- **protecting remote web-based staff agent sessions (in conjunction with HTTPS)**
- **protecting internal data transfer between the Management console (Control Server component) and the Core Server component (part of the Device Server component)**

When acting as a TLS client:

- **protecting audit records exported to an external audit server**
- **protecting the communication channel between the MDM Server and LDAP server for authentication**
- **protecting the communication channel between the MDM Server and a remote database server hosting the MDM Server's SQL database**

When acting as a TLS server and as a TLS client:

- **protecting internal data transfer between the Management console (Control Server, acting as TLS client) and the Core Server component (part of the Device Server, acting as TLS server)**

in accordance with: **none**.

FTP_PRO.1.3 The TSF shall permit **itself (when acting as a client), its peer** to initiate communication via the trusted channel.

FTP_PRO.1.4 The TSF shall enforce the following rules for the trusted channel:

When acting as a TLS server, the MDM Server shall not establish a trusted channel if the client certificate is invalid.

When acting as a TLS client, the MDM Server shall not establish a trusted channel if the server certificate is invalid, with no exceptions.

FTP_PRO.1.5 The TSF shall enforce the following static protocol options:

When acting as a TLS server, the MDM Server

- **shall support mutual authentication using X.509v3 certificates,**
- **shall support session renegotiation, no session resumption or session tickets,**
- **shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1.**

When acting as a TLS client, the MDM Server

- **shall present the Supported Groups Extension in the Client Hello with the supported groups [secp256r1, secp384r1, secp521r1],**
- **shall support mutual authentication using X.509v3 certificates.**

FTP_PRO.1.6 The TSF shall negotiate one of the following protocol configurations with its peer:

When acting as a server:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 no other cipher suites

When acting as a client:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,

PPM Application note (FTP_PRO.1). The PP/ST author should model all necessary trusted channel protocols by FTP_PRO.1. If different protocols are used, the PP/ST author should iterate FTP_PRO.1.

6.1.43 FTP_PRO.2 Trusted channel establishment

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Authentication failures during channel establishment.

b) Basic: All authentication attempts.

FTP_PRO.2.1 The TSF shall establish a shared secret with its peer using one of the following mechanisms:

ECDHE using elliptic curves secp256r1, secp384r1, secp521r1 and no other curves.

FTP_PRO.2.2 The TSF shall authenticate **its peer, itself to its peer** using one of the following mechanisms: **authentication using X.509v3 certificates as defined by RFC 5280** and according to the following rules:

When acting as a TLS server:

- **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 one of the expected identifiers for the client.**

When acting as a TLS client:

- **The MDM Server shall verify that the presented identifier matches the reference identifier according to RFC 6125.**

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall not accept the certificate. Certificate validation rules to be implemented by the TSF:

- **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, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.**
- **The TSF shall validate that any CA certificate includes caSigning purpose in the key usage field.**
- **The TSF shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.**
- **The TSF shall validate the revocation status of the certificate using OCSP as specified in RFC 6960.**
- **The TSF shall validate the extendedKeyUsage field according to the following rules:**
  - **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.**
  - **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 EKU field.**

– **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 EKU field.**

The TSF shall require a unique certificate for each client device.

FTP_PRO.2.3 The TSF shall use **TLS KDF as defined in RFC 5246** to derive the following cryptographic keys from a shared secret: **bulk encryption keys (symmetric keys), MAC keys as defined in RFC 5246**.

PPM Application note (FTP_PRO.2). The PP/ST author should model all necessary trusted channel establishment by FTP_PRO.2. If different protocols are used, the PP/ST author should iterate FTP_PRO.2. To satisfy remaining open dependencies of FTP_PRO.2, the PP/ST author should include FCS_CKM.1 or FCS_CKM.2 in the PP/ST according to the actual key management related to the chosen trusted channel protocols.

6.1.44 FTP_PRO.3 Trusted channel data protection

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Failures when attempting to verify channel properties in FTP_PRO.3.2.

FTP_PRO.3.1 The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: **AES as specified by FCS_COP.1/AES**.

FTP_PRO.3.2 The TSF shall protect data in transit from modification using one of the following mechanisms:

AES in GCM mode as specified by FCS_COP.1/AES,

PPM Application note (FTP_PRO.3). The PP/ST author should model all necessary trusted channel data protection by FTP_PRO.3. If different protocols are used, the PP/ST author should iterate FTP_PRO.3.

6.1.45 FTP_TRP.1/EN Trusted path [iteration for enrolment of device agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Failures of the trusted path functions.

b) Minimal: Identification of the user associated with all trusted path failures, if available.

c) Basic: All attempted uses of the trusted path functions.

d) Basic: Identification of the user associated with all trusted path invocations, if available.

FTP_TRP.1.1/EN The TSF shall **use TLS as defined by FTP_PRO.1 to** provide a communication path between itself and remote device agents that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

FTP_TRP.1.2/EN The TSF shall permit remote device agents to initiate communication via the trusted path.

FTP_TRP.1.3/EN The TSF shall require the use of the trusted path for device enrolment services.

PP Application Note (FTP_TRP.1/EN). The device enrolment services itself are not in the scope of the TSF. Device agents can be identified and authenticated via the requirements of FIA_UID.1 and FIA_UAU.1 only after device enrolment. The ST author should therefore describe in the TOE summary specification how the identification of the device agent and the TOE is assured.

6.1.46 FTP_TRP.1/DA Trusted path [iteration for device agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Failures of the trusted path functions.

b) Minimal: Identification of the user associated with all trusted path failures, if available.

c) Basic: All attempted uses of the trusted path functions.

d) Basic: Identification of the user associated with all trusted path invocations, if available.

FTP_TRP.1.1/DA The TSF shall **use TLS as defined by FTP_PRO.1 to** provide a communication path between itself and remote authorised device agents that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

FTP_TRP.1.2/DA The TSF shall permit remote authorised device agents to initiate communication via the trusted path.

FTP_TRP.1.3/DA The TSF shall require the use of the trusted path for initial user authentication, and mobile device management.

6.1.47 FTP_TRP.1/SA Trusted path [iteration for staff agents]

The following actions should be auditable (minimum or basic level of audit):

a) Minimal: Failures of the trusted path functions.

b) Minimal: Identification of the user associated with all trusted path failures, if available.

c) Basic: All attempted uses of the trusted path functions.

d) Basic: Identification of the user associated with all trusted path invocations, if available.

FTP_TRP.1.1/SA The TSF shall **implement HTTPS compliant with RFC 2818 using TLS as defined by FTP_PRO.1 to** provide a communication path between itself and remote authorised staff agents that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

FTP_TRP.1.2/SA The TSF shall permit remote authorised staff agents to initiate communication via the trusted path.

FTP_TRP.1.3/SA The TSF shall require the use of the trusted path for initial user authentication, and all services provided to authorised staff agents.

6.2 Security functional requirements rationale

6.2.1 Coverage

The following table provides a mapping of SFR components to the security objectives for the TOE, showing that each SFR component addresses at least one security objective and that all security objectives are addressed by one or more SFR components.

SFR component	OT.COMMUNICATION	OT.DEVICELIFECYCLE	OT.DEVICETRACKING	OT.LOGGING	OT.MANAGEMENT	OT.SEPARATION	OT.STORAGE	OT.TRUSTED-COMMUNICATIONCHANNEL
FAU_GEN.1			x	x				
FAU_GEN.2			x	x				
FAU_SAR.1			x	x				
FAU_SAR.2			x	x				
FAU_SAR.3			x					
FAU_STG.4			x	x				
FCS_CKM.1/ECDSA, /RSA								x
FCS_CKM.2/ECDHE								x
FCS_CKM.5/SYMM, /MAC								x
FCS_CKM.6								x
FCS_COP.1/AES, /RSA, /ECDSA, /SHA, /HMAC								x
FCS_RNG.1								x
FDP_IFC.1					x			
FDP_IFF.2					x			
FDP_ITT.1X					x			
FDP_RIP.1							x	
FDP_SDC.1							x	
FDP_SDI.1							x	
FDP_UCT.1						x		
FDP_UIT.1						x		
FIA_ATD.1		x	x	x	x	x		
FIA_UAU.1/DA			x		x	x		
FIA_UAU.1/SA		x	x	x	x	x		
FIA_UID.1/DA			x		x	x		
FIA_UID.1/SA		x	x	x	x	x		
FIA_USB.1					x	x		
FMT_MOF.1		x						
FMT_MSA.1					x			

SFR component	OT.COMMUNICATION	OT.DEVICELIFECYCLE	OT.DEVICETRACKING	OT.LOGGING	OT.MANAGEMENT	OT.SEPARATION	OT.STORAGE	OT.TRUSTED-COMMUNICATIONCHANNEL
FMT_MSA.3					x			
FMT_SMF.1/AD		x						
FMT_SMF.1/AU			x	x				
FMT_SMF.1/MA			x					
FMT_SMR.1		x	x	x	x			
FPT_ITT.1					x			
FTP_ITC.1	x							
FTP_PRO.1								x
FTP_PRO.2								x
FTP_PRO.3	x							x
FTP_TRP.1/EN		x						
FTP_TRP.1/DA	x					x		
FTP_TRP.1/SA	x					x		

Table 13: Mapping of SFR components to security objectives for the TOE

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives. The rationale has been taken from [MDMTSPP] and [TCCPPM].

Security Objective	Rationale how the SFRs are meeting the security objective
OT.COMMUNICATION	The objective OT.COMMUNICATION is met as follows: Provision of mutually authenticated trusted communication paths as required by FTP_TRP.1/SA and FTP_TRP.1/DA prevents unauthorised disclosure and modification of data exchanged between parts of the TOE and remote authorised device/staff agents as external entities.

Security Objective	Rationale how the SFRs are meeting the security objective
	FTP_PRO.3[17] ensures that the protection of confidentiality and integrity is based on the use of mutually authenticated trusted communication channels. Provision of mutually authenticated trusted communication channels required by FTP_ITC.1 prevents unauthorised disclosure and modification of data exchanged between parts of the TOE and remote authorised IT endpoints, i.e. secure LDAP server, external audit server.
OT.DEVICELIFECYCLE	The objective OT.DEVICELIFECYCLE is met as follows: The device enrolment services are protected by providing a trusted communication path as required by FTP_TRP.1/EN. This enforces a trusted identification of the enrolled device and prevents unauthorised disclosure and modification of data. All device life-cycle management activities are controlled by authorised administrator agents only, as required by FMT_SMF.1/AD, FMT_MOF.1 and FMT_SMR.1. The authorisation of administrator agents is required prior to any management action by FIA_UID.1/SA (staff agent identification), FIA_UAU.1/SA (staff agent authentication) and FIA_ATD.1 (definition of attribute role).
OT.DEVICETRACKING	The objective OT.DEVICETRACKING is met as follows: FAU_GEN.1 identifies, among others, all auditable events concerning the management activities of mobile devices. The auditable events are either listed in the requirements that define the MDM grouping SFP, or explicitly defined (life-cycle, configuration changes). In case the size of record data is limited, and to avoid data loss, FAU_STG.4 describes the actions to be taken if the size limit of the record is reached. FAU_GEN.2 makes sure that the device agent who caused an auditable event is identified in each audit record. FIA_UAU.1/DA and FIA_UID.1/DA make sure that device agents are successfully identified and authenticated before they can perform any operations that have an influence on their respective mobile devices' life cycles. The requirements FAU_SAR.1, FAU_SAR.2, FMT_SMF.1/AU and FMT_SMF.1/MA define the staff agents that are allowed to read audit information. FAU_SAR.1 and FAU_SAR.3 distinguish

[17] The rationale for FTP_PRO.3 has been taken from [TCCPPM].

Security Objective	Rationale how the SFRs are meeting the security objective
	between the roles and hierarchical groupings for which reading of audit information is allowed for the respective staff agents. The corresponding security attributes of staff agents (role and cluster of groupings) and device agents (grouping) are defined in FIA_ATD.1. The association of roles to staff agents is covered by FMT_SMR.1. FIA_UAU.1/SA and FIA_UID.1/SA make sure that staff agents are successfully identified and authenticated before they gain read access to audit information.
OT.LOGGING	The objective OT.LOGGING is met as follows: FAU_GEN.1 identifies, among others, all auditable events concerning the actions of staff agents. In case the size of record data is limited, and to avoid data loss, FAU_STG.4 describes the actions to be taken if the size limit of the record is reached. FAU_GEN.2 makes sure that the staff agent who caused an auditable event is identified in each audit record. The requirements FAU_SAR.1, FAU_SAR.2 and [AU]FMT_SMF.1 define that auditor agents are allowed to read all audit information. The corresponding security attribute role is defined in FIA_ATD.1. The association of roles to staff agents is covered by FMT_SMR.1. FIA_UAU.1/SA and FIA_UID.1/SA make sure that staff agents are successfully identified and authenticated.
OT.MANAGEMENT	The objective OT.MANAGEMENT is met as follows: The secure management of mobile devices is concerned with the management functions that can be initiated on behalf of manager agents and executed on behalf of device agents. FMT_SMR.1 specifies the role manager and it associates roles with staff agents. The security attributes of staff agents (role and cluster of groupings) and device agents (grouping) are identified in FIA_ATD.1. Staff agents (FIA_UAU.1/SA and FIA_UID.1/SA) and device agents (FIA_UAU.1/DA and FIA_UID.1/DA) are supposed to be identified and authorised before they can perform any action. FIA_USB.1 makes sure that staff attendants inherit the security attributes from their respective staff agents. FDP_IFC.1 identifies the *MDM grouping SFP*, the information flow control policy that monitors the operation of the management functions specified in Table 12. By FDP_IFF.2 the scope of control of the *MDM grouping SFP* is defined. It restricts device management functions to be initiated by manager attendants and executed by device attendants

Security Objective	Rationale how the SFRs are meeting the security objective
	based on a hierarchical relationship between their respective groupings. Changing the information security attribute 'cluster of groupings' is restricted to manager agents according to FMT_MSA.1 and FMT_MSA.3. Protection from unauthorised disclosure and modification is ensured by FDP_ITT.1X and FPT_ITT.1 when user and TSF data is exchanged between staff attendants and device attendants.
OT.SEPARATION	The objective OT.SEPARATION is met as follows: FIA_ATD.1 defines the security attributes for device agents and manager agents, whereas FIA_USB.1 binds the corresponding subjects (device attendants and manager attendants) to the respective agents. FIA_UID.1/SA and FIA_UAU.1/SA guarantee that manager agents are identified and authenticated before they can communicate with the manager attendant. Similarly, [DA]FIA_UID.1 and FIA_UAU.1/DA guarantee that device agents are identified and authenticated before they can communicate with device attendants. The protection of user data against unauthorised disclosure or modification is ensured by FDP_UCT.1 and FDP_UIT.1, both relying on separate trusted communication paths for staff agents (FTP_TRP.1/SA) and device agents (FTP_TRP.1/DA).
OT.STORAGE	The objective OT.STORAGE is met as follows: This objective essentially concerns user data requiring special protection. Confidentiality is ensured by FDP_SDC.1, and integrity is guaranteed by FDP_SDI.1. In addition, FDP_RIP.1 prevents residual information from reuse.
OT.TRUSTEDCOMMUNICATIONCHANNEL	The objective OT.TRUSTEDCOMMUNICATIONCHANNEL is met as follows:[18] FTP_PRO.1, FTP_PRO.2 and FTP_PRO.3 provide mutually authenticated trusted communication channels by using trusted channel protocols based on cryptographic mechanisms. FTP_PRO.1 ensures that communication be established in accordance with a defined protocol. FTP_PRO.2 ensures that keys be securely established between the peers using appropriate cryptographic mechanisms (FCS_COP.1/*) and appropriate cryptographic key generation (FCS_CKM.1/ECDSA, /RSA), cryptographic key distribution (FCS_CKM.2/ECDHE), cryptographic key

[18] This rationale has been taken from [TCCPPM].

Security Objective	Rationale how the SFRs are meeting the security objective
	derivation (FCS_CKM.5/SYMM, /MAC), cryptographic key destruction (FCS_CKM.6) and random number generation (FCS_RNG.1). FTP_PRO.3 ensures that data in transit be protected from unauthorised disclosure and modification using appropriate cryptographic operations (FCS_COP.1).

6.2.3 Justification of SFR dependencies

The following table provides justification for the dependencies of the SFR components, showing that all dependencies of the SRF components are satisfied, not applicable (void) or addressed by security objectives for the operational environment.

SFR component	Dependencies	Justification
FAU_GEN.1	FPT_STM.1	OE.RELIABLETIMESTAMPS; reliable timestamps will be provided by the operational environment.
FAU_GEN.2	FAU_GEN.1	satisfied
	FIA_UID.1	satisfied [iterations for device/staff agents]
FAU_SAR.1	FAU_GEN.1	satisfied
FAU_SAR.2	FAU_SAR.1	satisfied
FAU_SAR.3	FAU_SAR.1	satisfied
FAU_STG.4	FAU_STG.2	OE.AUDITTRAIL; the protection required for the audit trail will be provided by the operational environment
FCS_CKM.1/ECDSA, /RSA	FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1	satisfied by FCS_CKM.5 and FCS_COP.1
	FCS_CKM.3	not satisfied; key access as required by FCS_CKM.3 focuses on functions like key backup/recovery, key escrow, key import,... These functionalities are not required by the TOE to provide the security functions defined in this ST.
	FCS_RBG.1 or FCS_RNG.1	satisfied by FCS_RNG.1
	FCS_CKM.6	satisfied
FCS_CKM.2/ECDHE	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5	satisfied by FCS_CKM.1/ECDSA, FCS_CKM.1/RSA and FCS_CKM.5
	FCS_CKM.3	not satisfied; key access as required by FCS_CKM.3 focuses on functions like key backup/recovery, key escrow, key import,... These functionalities are not

SFR component	Dependencies	Justification
		required by the TOE to provide the security functions defined in this ST.
FCS_CKM.5/SYMM	FCS_CKM.2 or FCS_COP.1	satisfied by FCS_CKM.2
	FCS_CKM.6	satisfied
FCS_CKM.5/MAC	FCS_CKM.2 or FCS_COP.1	satisfied by FCS_CKM.2
	FCS_CKM.6	satisfied
FCS_CKM.6	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	satisfied by FCS_CKM.1
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5	satisfied by FCS_CKM.1 and FCS_CKM.5
	FCS_CKM.3	not satisfied; key access as required by FCS_CKM.3 focuses on functions like key backup/recovery, key escrow, key import,... These functionalities are not required by the TOE to provide the security functions defined in this ST.
FCS_RNG.1	No dependencies	–
FDP_IFC.1	FDP_IFF.1	satisfied by FDP_IFF.2 (hierarchical to FDP_IFF.1)
FDP_IFF.2	FDP_IFC.1	satisfied
	FMT_MSA.3	satisfied
FDP_ITT.1X	FDP_ACC.1 or FDP_IFC.1	satisfied by FDP_IFC.1
FDP_RIP.1	No dependencies	–
FDP_SDC.1	No dependencies	–
FDP_SDI.1	No dependencies	–
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1	satisfied by FTP_TRP.1
	FDP_ACC.1 or FDP_IFC.1	satisfied by FDP_IFC.1
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1	satisfied by FDP_IFC.1
	FTP_ITC.1 or FTP_TRP.1	satisfied by FTP_TRP.1
FIA_ATD.1	No dependencies	–
FIA_UAU.1/DA	FIA_UID.1	satisfied [iteration for device agents]
FIA_UAU.1/SA	FIA_UID.1	satisfied [iteration for staff agents]
FIA_UID.1/DA	No dependencies	–

SFR component	Dependencies	Justification
FIA_UID.1/SA	No dependencies	–
FIA_USB.1	FIA_ATD.1	satisfied
FMT_MOF.1	FMT_SMR.1	satisfied
	FMT_SMF.1	satisfied by FMT_SMF.1/AD
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	satisfied by FDP_IFC.1
	FMT_SMR.1	satisfied
	FMT_SMF.1	satisfied by FMT_SMF.1/MA
FMT_MSA.3	FMT_MSA.1	satisfied
	FMT_SMR.1	satisfied
FMT_SMF.1/AD	No dependencies	–
FMT_SMF.1/AU	No dependencies	–
FMT_SMF.1/MA	No dependencies	–
FMT_SMR.1	FIA_UID.1	satisfied by FIA_UID.1/SA
FPT_ITT.1	No dependencies	–
FTP_ITC.1	No dependencies	-
FTP_PRO.1	FTP_PRO.2	satisfied
	FTP_PRO.3	satisfied
FTP_PRO.2	FTP_PRO.1	satisfied
	FCS_CKM.1 or FCS_CKM.2	satisfied by FCS_CKM.1
	FCS_CKM.5	satisfied
	FCS_COP.1	satisfied
FTP_PRO.3	FTP_PRO.1	satisfied
	FTP_PRO.2	satisfied
	FCS_COP.1	satisfied
[EN]FTP_TRP.1	No dependencies	–
[DA]FTP_TRP.1	No dependencies	–
[SA]FTP_TRP.1	No dependencies	–

Table 14: Justification of SFR dependencies

6.3 Security assurance requirements

The security assurance requirements (SARs) of this Security Target are those defined by the [MDMTSPP] component of the PP-Configuration [MDMTSPPC].[19] They correspond to the assurance level EAL4 augmented with systematic flaw remediation ALC_FLR.3.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

[19] [TCCPPM] does not define additional SARs.

6.4 Security assurance requirements rationale

This Security Target adopts the security assurance requirements (SARs) defined by the [MDMTSPP] component of the PP-Configuration [MDMTSPPC]. An explanation of why these SARs were chosen can be found in [MDMTSPP].

Dependencies within the selected SARs have been considered by the authors of [MDMTSPP] and are not analysed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

7 TOE SUMMARY SPECIFICATION

The TOE summary specification identifies the security functions that the TOE implements to meet the security functional requirements defined in section 6.1 of this ST.

The table below shows which SFRs are satisfied by each of the TSFs.

SFR component	SF.AUDIT	SF.CRYPTO	SF.DP	SF.IA	SF. MGMT	SF. PT	SF. CHANNEL
FAU_GEN.1	x						
FAU_GEN.2	x						
FAU_SAR.1	x						
FAU_SAR.2	x						
FAU_SAR.3	x						
FAU_STG.4	x						
FCS_CKM.1/ECDSA		x					
FCS_CKM.1/RSA		x					
FCS_CKM.2/ECDHE		x					
FCS_CKM.5/SYMM		x					
FCS_CKM.5/MAC		x					
FCS_CKM.6		x					
FCS_COP.1/AES		x					
FCS_COP.1/RSA		x					
FCS_COP.1/ECDSA		x					
FCS_COP.1/SHA		x					
FCS_COP.1/HMAC		x					
FCS_RNG.1		x					
FDP_IFC.1			x				
FDP_IFF.2			x				
FDP_ITT.1X			x				
FDP_RIP.1			x				
FDP_SDC.1			x				
FDP_SDI.1			x				
FDP_UCT.1			x				
FDP_UIT.1			x				
FIA_ATD.1				x			
FIA_UAU.1/DA				x			

SFR component	SF.AUDIT	SF.CRYPTO	SF.DP	SF.IA	SF. MGMT	SF. PT	SF. CHANNEL
FIA_UAU.1/SA				x			
FIA_UID.1/DA				x			
FIA_UID.1/SA				x			
FIA_USB.1				x			
FMT_MOF.1					x		
FMT_MSA.1					x		
FMT_MSA.3					x		
FMT_SMF.1/AD					x		
FMT_SMF.1/AU					x		
FMT_SMF.1/MA					x		
FMT_SMR.1					x		
FPT_ITT.1						x	
FTP_ITC.1							x
FTP_PRO.1							x
FTP_PRO.2							x
FTP_PRO.3							x
FTP_TRP.1/EN							x
FTP_TRP.1/DA							x
FTP_TRP.1/SA							x

Table 15: SFRs met by the TSFs

7.1 SF.AUDIT - Security Audit

FAU_GEN.1 / FAU_GEN.2: The UEM Server automatically generates audit records for all required events specified in the SFR without any additional administrator configuration. The audit records are stored in the UEM Server's SQL database. The minimum set of audit records that can be generated are listed in **Table 9** along with:

- Start-up and shutdown of the audit functions by logging the start-up and shutdown of the MDM Server
- device enrolment / unenrolment
- configuration changes of mobile devices regarding
  - installed certificates
  - device settings
  - operating system version / patch level

- installed applications incl. version

Each event in the TOE's audit log includes a date/time stamp obtained from the host server (connected to an NTP server), event type and category, user, host, and a success indicator.

Each audit event resulting from an action of an identified user is associated with the identity of that user, i.e. the username in case of administrative actions performed by staff members, a UUID (internal unique device ID) in case of actions performed by a device agent.

FAU_SAR.1: The UEM Server collects, protects, and can display audit messages to authorized auditors and managers. As the UEM Server generates audit events it stores them within its SQL database. Those events are available to be viewed via the UEM Server administrator portal. Periodically, the audit events stored in the SQL database are also forwarded to a configured SYSLOG server where they can be viewed in the operational environment.

Note that audit events collected from enrolled mobile devices are received and immediately forwarded to a configured SYSLOG server where they can be examined. The UEM Server does not provide any interface to view these audit events and thus the functions from the environment are invoked to read audit data from the SYSLOG server.

FAU_SAR.2: The TOE implements role-based access control. Only administrative users associated with roles that have access rights to access audit information can access them. Mobile devices and users who do not have this permission are not provided a mechanism to view audit data.

FAU_SAR.3: The Management console of the UEM Server supports filtering of audit data based on the attributes 'Source', 'Role', 'Category', 'Action', 'Sub-category' and 'Policy category'. If filters are applied, the Management console displays audit data that matches all of the selected filters.

FAU_STG.4: The UEM Server stores audit data in the same SQL database where most of its configuration data is stored. The BlackBerry UEM Administrative Guidance Document defines SQL Server settings for the database that ensure that within the configurable lifetime of 1 to 365 days the audit storage cannot be exceeded.

7.2 SF.CRYPTO - Cryptographic Support

FCS_CKM.1/*, FCS_CKM.2/*, FCS_COP.1/*: The UEM Server uses its Certicom Security Builder GSE-J Crypto Core (version 2.9.2) to generate asymmetric RSA keys for authentication and key establishment. The UEM Server issues its own RSA 3072-bit certificates and stores them into the UEM Server SQL database so that they can be shared by distributed UEM Server instances.

The UEM Server provides ECDSA key generation using P-256, P-384 and P-521 curves in support of ECDHE key establishment.

The UEM Server handles decryption errors in accordance with NIST Special Publication 800-56B. It does not reveal the particular error that occurred, either through the contents of any outputted or logged error message or through timing variations.

Vector testing, leveraging the NIST Automatic Cryptographic Validation Protocol (ACVP) demo server, using Certicom Security Builder GSE-J Crypto Core version 2.9.2 has been performed for the algorithms listed in the table below.

Requirement	Function	Details
FCS_CKM.1/*	RSA and ECDSA key generation	RSA 186-4: Key(gen) – 3072 bit ECDSA 186-4: Key(gen) P256, P-384, P-521
FCS_CKM.2/*	Key Agreement: KAS ECC schemes; KA Role Initiator and responder	KAS ECC: Ephemeral Unified, KaRole(initiator, responder)

Requirement	Function	Details
FCS_COP.1/*	Encryption/decryption	AES 128/256 CBC AES 128/256 GCM
	Cryptographic signature generation/verification	RSA SigGen(3072), SigVer(3072)
		ECDSA PKG/PKV/SigGen/SigVer P-256, P384, P-521
	Cryptographic hashing	SHA-256/384/512
	keyed-hash message authentication	HMAC SHA-256/384
FCS_RNG.1	DRBG	Hash_DRBG (any)

Table 16: Crypto Algorithms

The UEM Server (using its Certicom library) generates and verifies RSA (using 3072 bits) and ECDSA (using P-256, P-384, and P-521 curves) signatures, performs HMAC-SHA hashing, performs AES encryption and decryption, performs SHA hashing, establishes TLS/HTTPS connections, generates IVs, and generates random data.

The UEM Server utilizes these cryptographic algorithms primarily during establishment of TLS/HTTPS connections (which require signature generation and verification as part of peer authentication, hashing as part of the signatures for peer authentication and for HMAC integrity, HMAC for integrity of the trusted channel, AES for the confidentiality of the trusted channel, and RBGs to generate nonces and IVs) and for the generation of random numbers.

When using HMAC as part of TLS, the UEM Server utilizes HMAC keys equal to the block size of the underlying hash algorithm. Thus, when employing HMAC-SHA-256, the UEM Server uses a 32-byte key to generate a 32-byte hash. Likewise, when employing HMAC-SHA-384, it uses a 48-byte key when performing hashing to produce a 48-byte hash.

The UEM Server generates IVs for AES CBC and AES GCM using unpredictable (random) IVs drawn from the Hash_DRBG (any) (which meets the “unpredictable” requirement of SP 800-38A and SP800-38D).

FCS_CKM_5/*: The UEM Server derives symmetric keys and MAC keys required for the TLS data encryption and message authentication as defined in RFC 5246.

FCS_CKM_6: The UEM Server clears plaintext keys (TLS and HTTPS session keys) from memory after those keys are no longer needed.

Note that the UEM Server stores certificates and the related private keys (the only persistently stored keying material) in its SQL database in encrypted format, and when any new certificates are generated or imported, the UEM Server will directly overwrite the old keys with the new in the encrypted key store in the SQL database.

FCS_RNG.1: The UEM Server is using the Hash_DRBG with a SHA2-512 core provided by the underlying Certicom library. The UEM Server utilizes Jitter RNG version 3.0.0 to seed its DRBG. Analysing the raw noise data generated by Jitter RNG 3.0.0 on the ST hardware confirmed that each bit of output provides 1 bit of entropy. The UEM Server is designed to ensure that if the entropy source delivers at least 0.666 bits of entropy per bit of output, the DRBG will be properly seeded with a minimum of 256 bits of entropy.

7.3 SF.DP – User Data Protection

FDP_SDC.1: The UEM Server uses certificates to provide an internal PKI which supports the issuance of certificates for its own use (i.e., to identify itself to other parties) and to be sent to mobile devices during enrolment. Private keys of certificates used by the UEM Server are stored encrypted in the server's SQL database (AES-GCM mode) using a 256-bit DEK (data encryption key) created during installation. The DEK is encrypted (AES-CBC mode with HMAC-SHA-256 as an integrity check) using a 256-bit KEK (key encryption key) created during installation. The encrypted DEK is stored in the local file system of each unit of scale. The KEK is stored in and protected by the Windows key store. At no time does the UEM Server store any plaintext keys, plaintext PINs and plaintext passwords on its hard drive or its SQL database. The UEM Server does not store any ephemeral keys (e.g., TLS/HTTPS session keys).

FDP_IFC.1: The MDM Server implements the grouping of devices and assignment of these groups to different managers by assigning different parameters to a device. While UEM supports a wide variety of parameters, for the TOE the parameters Operating System (OS), Operating System Version (OSV), Device Model (DM) and Manufacturer (M) have been selected. For a definition of the bounded sub-lattices, see the SFR FDP_IFC.1. For each device any of the parameters listed above has a dedicated value, e.g. a device does not run two different OS Versions at the same time.

FDP_IFF.2 / FDP_UIT.1: Mobile device management function payloads are transferred over the air to mobile devices, using a secure TLS channel (FTP_TRP.1/DA). Payloads (i.e. new or updated policies and commands) are sent to the MDM agent during its next check-in to the UEM Server. The UEM Server uses predefined rules to determine applicable commands and policies to be sent to mobile devices. The UEM server also takes the mobile device's capabilities into account; it only transfers commands and policies that the device is able to apply.

Each device policy is signed by the UEM server using an RSA certificate issued for that purpose. It is then sent to the device agent via a secure TLS channel according to FTP_TRP.1/DA.

Enrolled mobile devices are periodically notified by the Core Server via APNs or FCM depending on the operating system of the mobile device to check-in with a configurable interval. Managers can also initiate an immediate check-in using the UEM Server's Management console.

FDP_ITT.1X: User data transmitted between the Management console (control server component) and the Core Server component (part of the device server component) is protected against unauthorized disclosure and modification through the use of HTTPS TLS version 1.2 (RFC 5246) with mutual certificate-based authentication as defined by FTP_PRO.1, FTP_PRO.2 and FTP_PRO.3. The Management console is the TLS client, the Core Server component is the TLS server in this case.

FDP_RIP.1: The residual information that needs to be protected from unauthorized re-use in the context of the MDM grouping SFP are PINs and passwords entered by users for authentication to the TOE as well as ephemeral keys for TLS sessions. Plaintext PINs and passwords sent to the TOE for user authentication and reference values retrieved from the database are erased from the database storage after the user is deleted, or before it is updated, using the Java AutoCloseable function and overwriting the data with zeros. Ephemeral keys for TLS sessions are erased from volatile memory as stated by FCS_CKM.6.

FDP_SDI.1: The UEM Server stores user passwords, PINs, passwords used for key derivation as well as X509v3 certificates and related private keys encrypted in its SQL database, using AES-256 GCM

FDP_UCT.1: User data is protected against unauthorised disclosure and modification by transmitting data via the trusted communication paths for staff agents (FTP_TRP.1/SA) and device agents (FTP_TRP.1/DA).

7.4 SF.IA - Identification and authentication

FIA_ATD.1: The UEM Server stores the following attributes for administrative user accounts: role (including permissions) assigned to the administrative user; mobile device users and user groups managed by the administrative user. For mobile devices enrolled in the UEM Server, the UEM Server stores the mobile device user who activated the device and the device group to which the mobile device has been assigned.

FIA_UAU.1/DA, FIA_UID.1/DA: During the enrollment process, LDAP credentials are used to activate a mobile device over a secure TLS channel between the agent on the mobile device and the UEM Server. The UEM Server, having authenticated to the device agent through presentation of its certificate during the TLS handshake, checks that the LDAP credentials are valid. Once the enrollment process has completed, all subsequent connections between the device agent and the UEM Server occur through a mutually authenticated TLS session (in which the device agent presents its certificate to the UEM Server).

FIA_UAU.1/SA, FIA_UID.1/SA: The UEM Server allows staff members to request password recover, choose a language and select the authentication provider before requiring that any staff member connecting to the server authenticate by providing a username and password. Put another way, a staff member cannot perform any actions at all (other than logging in, requesting password recover, choosing a language and selecting the authentication provider) until the staff member successfully authenticates.

FIA_USB.1: The MDM server associates roles and permissions (i.e. a cluster of groupings) as security attributes with staff agents and groupings as security attributes with device agents via the TOEs role-based access control.

The TOE supports the creation of local users, but also allows to use users maintained in an LDAP server. In the latter case, the TOE handles user data that is synchronized with LDAP. This user data cannot be directly modified on the TOE but only updated by modifying the data on LDAP and synchronizing with LDAP afterwards. Users, user attributes and group membership are maintained in LDAP.

There is additional user data that is not maintained by LDAP and that can directly be modified on the TOE. Roles with permissions are maintained in the MDM-TS directly and not LDAP.

All changes to the user data are audited.

7.5 SF.MGMT - Security management

FMT_SMR.1, FMT_SMF.1/AD, FMT_SMF.1/AU, FMT_SMF.1/MA: The UEM Server provides a set of preconfigured roles and allows for the creation of custom roles. The evaluated configuration of the TOE has at least the following roles:

Role	Tasks defined by SFRs	Description
Server primary administrator	-	Server primary administrators are administrators that have an administrative account on the underlying Microsoft Windows Server platform (i.e., the Windows administrator), log into Windows locally or through RDP, and are responsible for installation, install configuration, and have access to the SQL server database associated with the UEM Server.

Role	Tasks defined by SFRs	Description
Security Administrator		Security administrators log into the UEM Server's HTTPS WebUI (Management console) and are responsible for configuring the UEM Server's settings. The Security Administrator role has full permissions to the management console, including creating and managing roles and administrative users. There must be at least one Security Administrator.
Administrator	See FMT_SMF.1/AD	Administrators (in the sense of [MDMTSPP]) login through the UEM Server's HTTPS WebUI and have the permissions required to complete the tasks specified in section 6.1.36.
Auditor	See FMT_SMF.1/AU	Auditors login through the UEM Server's HTTPS WebUI and have permissions only to access the UEM Server's audit log.
Manager	See FMT_SMF.1/MA	Managers login through the UEM Server's HTTPS WebUI and are responsible for managing (groups of) mobile devices and mobile device users. They have the permissions required to complete the tasks specified in section 6.1.38.
Mobile device users (MD users)	-	The UEM Server allows mobile device users to enroll their mobile devices using their LDAP credentials, and thus allows mobile device users to have the UEM Server manage their mobile devices to secure organization data and access.

Table 17: Roles supported by the TOE

All staff members (other than the server primary administrator) connect remotely to the UEM Server via HTTPS (using a standard web browser) and must be authenticated (providing a username and password) before gaining any access to the server. The UEM Server requires that administrator accounts be created for each staff member (and associated with existing roles or custom roles that can be configured by the Security Administrator to have a wide variety of permission combinations), and separates such staff members from mobile device users (unless a Security Administrator has explicitly created a separate administrative account for the user).

ST Application Notes (FMT_SMR.1). The roles "Mobile device user", "Server primary administrator", and "Security administrator" are listed in Table 17 for the sake of completeness as they are always present in the evaluated configuration of the TOE. However, no claims are made about these roles in this ST.

FMT_MOF.1, **FMT_MSA.1, FMT_MSA.3**: The MDM Server restricts all security management functions (identified above for FMT_SMF.1/AD, FMT_SMF.1/AU, FMT_SMF.1/MA) to an authorized

staff agent. This is accomplished by role-based access controls (described above) assigned to each of the management screens and the associated functions. Any single permission a user role should have needs to be explicitly assigned by the manager. So, a user has no permissions by default. This default behavior cannot be changed by the manager.

7.6 SF.PT - Protection of the TSF

FPT_ITT.1: The UEM Server consists of two components: the Management console (control server component) to service staff interactions and the Core Server component (part of the device server component) to service device interactions. The Management console securely communicates with the Core Server component through HTTPS TLS version 1.2 (RFC 5246) with mutual certificate-based authentication as defined by FTP_PRO.1, FTP_PRO.2 and FTP_PRO.3. The Management console is the TLS client, the Core Server component is the TLS server in this case.

7.7 SF.CHANNEL - Trusted path/channels

FTP_PRO.1, **FTP_PRO.2, FTP_PRO.3, FTP_ITC.1**: The UEM Server implements TLS to secure communication with all enrolled device agents, remote staff agents (in combination with HTTPS), a remote database server as well as external audit and LDAP authentication servers. Since the UEM Server provides the MAS server functionality, there is no additional communication path for the MAS audit communications. The UEM Server is a TLS client when communicating with a remote database server and the external audit and LDAP authentication servers.

The UEM Server supports TLS version 1.2 (RFC 5246). All versions of the SSL protocol and other versions of the TLS protocol are refused by the UEM Server.

The TLS for each of these channels is capable of supporting mutual authentication using X509v3 certificates, while mutual authentication is always required for enrolled device agents, as well as external audit and LDAP servers. The UEM Server will not establish a TLS session if the certificate presented by the peer is determined to be invalid.

The UEM Server uses its Certicom library to perform X509v3 certificate validation in conformance with FTP_PRO.2. It accepts the use of wildcards in the SAN or CN for all certificates received during a TLS session negotiation. The UEM Server performs hostname checking to ensure that the expected hostname matches the certificate Common Name or Subject Alternate Name (when the UEM Server validates the certificate from an LDAP or Syslog server). When the UEM server is accepting TLS communications from a device agent, the UEM server verifies the device agent's certificate by ensuring that that the Distinguished Name (DN) in the presented certificate matches a DN in a database of valid, known DNs.

For key exchanges, the UEM server supports ECDHE key exchanges with EC curves secp256r1, secp384r1, and secp521r1.

The UEM Server validates X509v3 certificates (including the full path) and checks their revocation status using OCSP. The server processes certificates presented during the TLS handshake by first checking the received certificate's validity period and appropriate key usage property. The server checks that it can construct a certificate path from the received certificate through any intermediary CAs to a trusted root CA. If the server can successfully build the certificate path, then it will next check the validity of the CA certificates (e.g., checking its validity dates and that the CA flag is present in the basic constraints section for all CA certs) in the chain. Assuming the server determines that all CA certificates in the chain are valid, it will finally check the revocation status of the received certificate against an OCSP server. The UEM Server will not accept a TLS/HTTPS certificate as valid in the event that it cannot contact the revocation server. The UEM Server will not accept any certificate for which it cannot determine the validity and will reject the connection

attempt. Note that the UEM Server only utilizes certificate pinning for communication between the MDM Server and enrolled iOS devices.

In the evaluated configuration, the UEM Server is configured with an X509v3 certificate to present during TLS negotiation with an audit (Syslog) server, an X509v3 certificate to present during TLS negotiation with an LDAP server. The certificates used by the UEM Server for these communication channels are independent from one another and from its internal certificates used for communication with mobile devices.

The UEM Server supports the following cipher suites when acting as a TLS client:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,

The UEM Server supports the following cipher suites when acting as a TLS server:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

FTP_TRP.1/EN: The UEM Server implements a TLS trusted communication channel according to FTP_PRO.1 for the communication with device agents during enrolment. The enrolment process is either initiated manually by the mobile device user or – in case of automated enrolment – by an enrolment-supporting service (DEP for iOS and KME for Android). The mobile device agent connects to the UEM Server using the URL provided by the mobile device user or configured at the enrolment service. It authenticates the UEM Server through the server's X.509 certificate. To be able to proceed with enrolment, the mobile device user needs to supply LDAP credentials. After successful verification of the user's credentials, the UEM server issues a device certificate to secure all future communication according to FTP_TRP.1/DA with the device agent.

FTP_TRP.1/DA: The UEM Server implements TLS according to FTP_PRO.1 to secure communication with all enrolled device agents. Mutual authentication using X.509 certificates (and certificate pinning for iOS) is always required for enrolled device agents.

FTP_TRP.1/SA: The UEM Server implements HTTPS as its trusted communication path for communications with authorised remote staff agents. Remote staff agents must connect to the UEM Server using HTTPS to securely administer the UEM Server. Remote staff agents can administer the UEM Server by using the BlackBerry Web Services APIs or by using a normal web browser to access the web UI. The legacy SOAP API must not be used in the evaluated configuration. The UEM Server provides no other mechanism or method beyond HTTPS for a remote staff agent to configure or access the UEM Server.

When accepting incoming HTTPS connections from remote staff agents, the UEM Server follows RFC 2818 and presents its server certificate. However, the UEM Server does not request that the remote staff agent present a certificate (in other words, the UEM Server does not require TLS mutual/client authentication for remote staff agents). Instead, the remote staff agent authenticates to the UEM Server using a username and password, transmitted to the UEM Server after they have established the TLS session.

8 REFERENCES

[AIS20] A proposal for: Functionality classes for random number generators, Version 2.0, 18. September 2011

[CC:2022] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, November 2022, CC:2022 Revision 1, CCMB-2022-11-001; Part 2: Security functional components, November 2022, CC:2022 Revision 1, CCMB-2022-11-002; Part 3: Security assurance components, November 2022, CC:2022 Revision 1, CCMB-2022-11-003.

[CC3.1R5] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; Part 2: Security functional components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002; Part 3: Security assurance components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[CEM:2022] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CC:2022 Revision 1, CCMB-2022-11-006.

[CEM3.1R5] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004.

[MDMTSPP] PP Mobile Device Management – Trusted Server (MDM-TS), BSI-CC-PP-0115, Version 1.0.

[MDMTSPPC] PP-Configuration Mobile Device Management – Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC), BSI-CC-PP-0116, Version 1.0.

[TCCPPM] PP-Module Trusted Communication Channel (TCC), registered as component of PP-Configuration BSI-CC-PP-0116, Version 1.0.

9 ABBREVIATIONS

CC	Common Criteria
ECIES	Elliptic Curve Integrated Encryption Scheme
EOL	End of Life
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Managements
PP	Protection Profile
PPM	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEM	Unified Endpoint Management
VM	Virtual Machine