Federal Office
for Information Security

Protection Profile
Mobile Device Management – Trusted Server (MDM-TS)

Common Criteria Protection Profile
BSI-CC-PP-0115, Version 1.0

Change history

Version	*Date*	*Description*
1.0	27.09.2021	Approved edition for initial release

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Phone: +49 22899 9582-0
E-Mail: mdm-pp@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of contents

List of figures

List of tables

1 PP Introduction

1.1 PP Reference

Title	Mobile Device Management – Trusted Server (MDM-TS)
Short title	PP MDM-TS
Version	1.0
Registration	BSI-CC-PP-0115
Editor/Sponsor	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI)
Author	IT Security Evaluation Laboratory at German Research Center for Artificial Intelligence (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH – DFKI)

1.2 Target of Evaluation (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.

1.2.1 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 may consist of several separated server components of the MDM system. Any client component of the MDM systems is outside of the TOE boundary. The TOE provides services to distribute data, applications, updates, as well as configuration commands and policy settings on mobile devices. Typically, both corporate and personal mobile devices are supported.

This PP conceptually considers two separated TOE components, the TOE device server component and the TOE control server component. This separation 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.

Application Note (TOE components). 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.

1.2.2 Usage and Major Security Features

The TOE device server component interacts with mobile devices and may be connected to some supporting non-TOE services, in particular enrolment, notification, inventory, 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 may be connected to some supporting non-TOE services, in particular inventory, logging, database and directory services. 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 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.

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.

In general, there is no restriction on the operational environment of the TOE. Some or all TOE components may be operated in the corporate IT infrastructure (on-premises) or in some separate cloud IT infrastructure (off-premises). In any case, care is to be taken regarding the security of transmitted and stored data.

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.

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.

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.

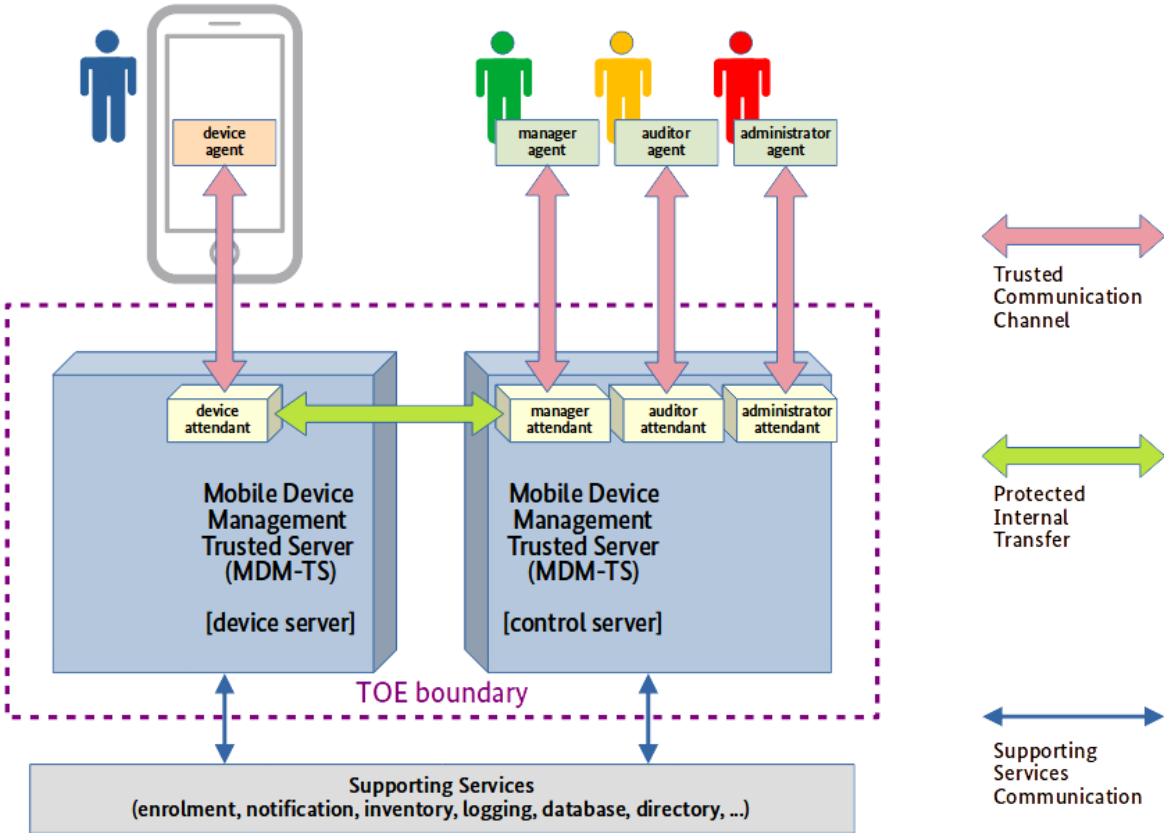


Figure 1: TOE boundary and environment

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. In particular, groupings enable multi-tenancy support, i.e. the TOE may serve multiple tenants by assigning every tenant a dedicated group of device/staff agents. The grouping concept is defined in terms of a bounded lattice, i.e., a mathematical structure on partially ordered sets with specific additional properties (see section 1.3).

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 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 appendix section 7.5.

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 including but not limited to 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 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.

1.2.3 Non-TOE Hardware/Software/Firmware

The TOE relies on non-TOE hardware/software for providing trusted communication channels based on cryptographic mechanisms to ensure confidentiality and integrity of data in transit between the TOE and authorised device/staff agents.

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.

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.

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.

1.3 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* (see appendix section 7 for some examples).
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*.

2 Conformance Claims

2.1 CC Conformance Claim

This PP claims conformance to Common Criteria Version 3.1 Revision 5 (CC 3.1R5):

- CC Part 2 extended with family FDP_SDC and component FDP_ITT.1X
- CC Part 3 conformant

2.2 PP Claim and Package Claim

This PP does not claim conformance to any other PP.

This PP claims to be EAL 4 augmented with ALC_FLR.3.

2.3 PP Conformance Statement

This PP requires strict conformance of any PP or ST claiming conformance to it.

The following PP-Modules can be specified in a PP-Configuration with this PP:

- PP-Module Trusted Communication Channel (TCC), Version 1.0

3 Security Problem Definition

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

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 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.

3.2 Organisational Security Policies

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 5. 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.

3.3 Assumptions

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.

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.

4 Security Objectives

4.1 Security Objectives for the TOE

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.

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 5. Management functions shall be performed only on behalf of authorised device agents or authorised manager agents. The 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.

4.2 Security Objectives for the Operational Environment

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 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 lifecycle. 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.TRUSTEDCOMMUNICATIONCHANNEL

The operational environment shall provide mutually authenticated trusted communication channels. The operational environment shall implement the trusted communication channels using trusted channel protocols based on cryptographic mechanisms.

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.

4.3 Security Objectives Rationale

All security objectives trace to threats and organisational security policies (see Table 1).

All security objectives for the operational environment trace to assumptions (see Table 2).

Tracing of security objectives to threats and organisational security policies	T.MALICIOUSDEVICE	T.MALICIOUSSTAFF	T.MASQUERADING	T.COMPROMISED-COMMUNICATION	T.COMPROMISED-STORAGE	P.SEPARATION	P.MANAGEMENT
OT.COMMUNICATION	×	×	×	×		×	
OT.DEVICELIFECYCLE	×	×					
OT.DEVICETRACKING	×						
OT.LOGGING		×					
OT.MANAGEMENT	×	×					×
OT.SEPARATION	×	×	×			×	
OT.STORAGE					×		
OE.PROPERSTAFF	×	×					×
OE.PROPERUSER	×						×
OE.PROPERMANAGEMENT							×
OE.RESILIENCE							×
OE.DEVICELIFECYCLE	×						×
OE.SUPPORTINGSERVICES	×	×	×		×		×
OE.TRUSTEDCOMMUNICATIONCHANNEL	×	×	×	×		×	
OE.RELIABLETIMESTAMPS	×	×					
OE.AUDITTRAIL		×					

Table 1: Tracing of security objectives to threats and organisational security policies

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, OE.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, OE.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 OE.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 OE.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 OE.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.

Tracing of security objectives for the environment to assumptions	A.PROPERSTAFF	A.PROPERUSER	A.PROPERMANAGEMENT	A.RESILIENCE
OE.PROPERSTAFF	×			
OE.PROPERUSER		×		
OE.PROPERMANAGEMENT			×	
OE.RESILIENCE				×
OE.DEVICELIFECYCLE				
OE.SUPPORTINGSERVICES				
OE.TRUSTEDCOMMUNICATIONCHANNEL				
OE.RELIABLETIMESTAMPS				
OE.AUDITTRAIL				

Table 2: 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.

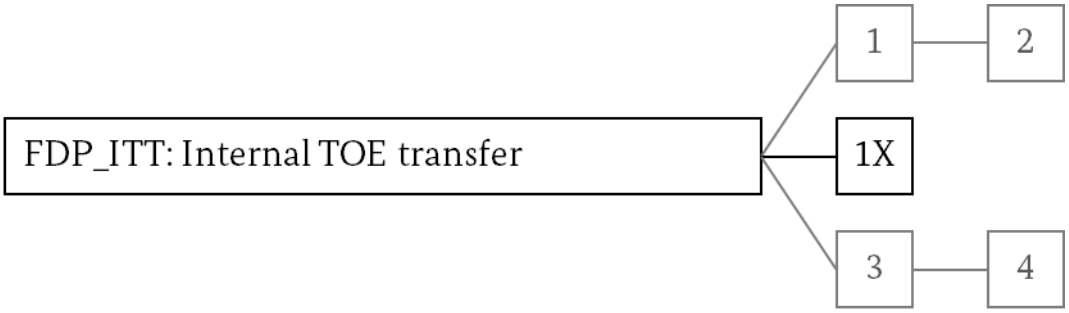
5 Extended Components Definition

5.1 Internal TOE transfer (FDP_ITT)

Family behaviour

See CC Part 2, Par. 201

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, Par. 202-205).

Management: FDP_ITT.1X

The following actions could 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 could provide a pre-defined role with the ability to select the method that will be used.

Audit: 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:

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 Simple internal transfer protection

Hierarchical to: No other components.

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

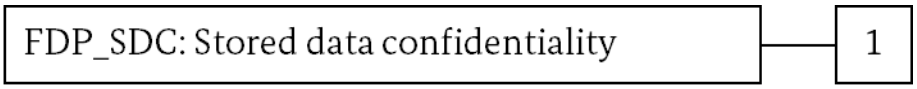
FDP_ITT.1X.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between separate parts of the TOE.

5.2 Stored Data Confidentiality (FDP_SDC)

Family behaviour

This family provides requirements that address protection of user data confidentiality while the data is stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family FDP_SDI *Stored data integrity* which protects the user data from integrity errors while being stored in the memory.

Component levelling



FDP_SDC.1 *Stored data confidentiality*, requires the TSF to protect the confidentiality of information of the user data in specified memory areas.

Management: FDP_SDC.1

There are no management activities foreseen.

Audit: FDP_SDC.1

There are no auditable events foreseen.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of [selection: all user data, the following user data [assignment: list of user data]] while it is stored in the [selection: temporary memory, persistent memory, any memory].

6 Security Requirements

6.1 Security Functional Requirements (SFRs)

The SFR components stated in this section are tailored through the use of permitted operations:

- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list;
- Refinement: allows the addition of details; and
- Iteration: allows a component to be used more than once with varying operations.

The tailoring through assignment, selection and refinement operations is explicitly identified in each SFR component by a tailoring table. This table indicates for each operation its consecutive number, its type (assignment, selection or refinement), the original phrase of the SFR element, and the tailoring phrase. The reproduction of the SFR elements refers to the tailoring by the consecutive numbers (superscripted in square brackets). The tailoring phrases are distinguished by italic font shape.

The tailoring through iteration operations is explicitly identified in each iterated SFR component by unique identifiers (superscripted in square brackets) in front of the short name of the SFR component.

Example (tailoring).
Assume a fictitious SFR component FOO_BAR.X with the following SFR element:

FOO_BAR.X.1 The TSF shall require each participant successfully authenticated before providing [selection: charming, stylish, glamorous] decorations for [assignment: list of celebratory events].

Two exemplary iterations of the fictitious SFR component would be explicitly identified as [ONE]FOO_BAR.X and [TWO]FOO_BAR.X.

An exemplary tailoring through assignment, selection and refinement operations on the fictitious SFR element would be explicitly identified by the following tailoring table.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	successfully authenticated	successfully authenticated *by a valid voucher*
[2]	selection	charming, stylish, glamorous	*charming and glamorous*
[3]	assignment	list of celebratory events	*the flower ceremony*

The tailored SFR element of the exemplary iteration [ONE] would be reproduced as follows:

[ONE]FOO_BAR.X.1 The TSF shall require each participant successfully authenticated [1]*by a valid voucher* before providing [2]*charming and glamorous* decorations for [3]*the flower ceremony*.

6.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	choose one of: minimum, basic, detailed, not specified	*basic*
[2]	refinement (editorial)	and c) [assignment: other specifically defined auditable events]	c) *[assignment: other specifically defined auditable events]; and* d) *[assignment: other specifically defined auditable events]*
[3]	assignment	other specifically defined auditable events	*device enrolment, device unenrolment and [assignment: other auditable events in the life-cycle of mobile devices]*
[4]	assignment	other specifically defined auditable events	*configuration changes of mobile devices regarding* *i. installed certificates* *ii. device settings* *iii. operating system version / patch level* *iv. installed applications incl. version* *and [assignment: other configuration changes of mobile devices]*

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 [1]*basic* level of audit; [2]

c) [3]*device enrolment, device unenrolment and [assignment: other auditable events in the life-cycle of mobile devices]; and*

d) [4]*configuration changes of mobile devices regarding*

i. installed certificates

ii. device settings

iii. operating system version / patch level

iv. installed applications incl. version

and [assignment: 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 audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

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

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

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

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	authorised users	*authorised staff agents as specified in Table 3*
[2]	assignment	list of audit information	*the list of audit information as specified in Table 3*
[3]	refinement	user	*staff agent*

Authorised users	*List of audit information*
auditor agents, i.e. staff agents associated with role auditor	all 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 3: Audit review capabilities

FAU_SAR.1.1 The TSF shall provide [1]*authorised staff agents as specified in Table 3*, with the capability to read [2]*the list of audit information as specified in Table 3* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the [3]*staff agent* to interpret the information.

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

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 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.

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

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	methods of selection and/or ordering	*filtering*
[2]	assignment	criteria with logical relations	*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*

FAU_SAR.3.1 The TSF shall provide the ability to apply [1]*filtering* of audit data based on [2]*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.*

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.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.3.1 The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].

Application Note (FAU_STG.3). 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.

6.1.7 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	information flow control SFP	*MDM grouping SFP*
[2]	assignment	list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP	*the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 4*

FDP_IFC.1.1 The TSF shall enforce the [1]*MDM grouping SFP* on [2]*the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 4*.

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 5
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 5.

Table 4: 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
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
10)	Configure biometric authentication policy settings
11)	Configure push message policy settings
12)	Activate/Deactivate developer mode, e.g. Android Debug Bridge (ADB)
13)	Query software integrity attestation status incl. jailbreak / rooting detection
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)	Enable/Disable location services
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 5: Mobile Device Management Functions

Application Note (MDM functions). The MDM functions specified in Table 5 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.

6.1.8 FDP_IFF.2 Hierarchical security attributes

Hierarchical to: FDP_IFF.1 Simple security attributes.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	information flow control SFP	*MDM grouping SFP*
[2]	assignment	list of subjects and information controlled under the indicated SFP, and for each, the security attributes	*the list of subjects and information, and for each, the security attributes as defined in Table 4*
[3]	assignment	for each operation, the security attribute-based relationship that must hold between subject and information security attributes	*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*
[4]	assignment	additional information flow control SFP rules	*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*
[5]	assignment	rules, based on security attributes, that explicitly authorise information flows	*none*

Tailoring (assignment, selection, refinement operations on SFR elements):

[6]	assignment	rules, based on security attributes, that explicitly deny information flows	*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*
[7]	refinement (editorial)	(information flow control) security attribute(s)	*grouping(s)*
[8]	refinement	an ordering function	*a partial ordering relation with a unique minimum (bottom grouping) and a unique maximum (top grouping)*
[9]	refinement (editorial)	greater	*greater or lower*
[10]	refinement	"least upper bound"	*join function*
[11]	refinement	security attribute	*unique join grouping*
[12]	refinement	greater than or equal to	*the supremum (least upper bound) of*
[13]	refinement	"greatest lower bound"	*meet function*
[14]	refinement	security attribute	*unique meet grouping*
[15]	refinement	not greater than	*the infimum (greatest lower bound) of*

FDP_IFF.2.1 The TSF shall enforce the [1]*MDM grouping SFP* based on the following types of subject and information security attributes: [2]*the list of subjects and information, and for each, the security attributes as defined in Table 4*.

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: [3]*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 [4]*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: [5]*none*.

FDP_IFF.2.5 The TSF shall explicitly deny an information flow based on the following rules: [6]*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 [7]*groupings:*

a) There exists [8]*a partial ordering relation with a unique minimum (bottom grouping) and a unique maximum (top grouping)* that, given two valid [7]*groupings*, determines if the [7]*groupings* are equal, if one [7]*grouping* is [9]*greater or lower* than the other, or if the [7]*groupings* are incomparable; and

b) There exists a [10]*join function* in the set of [7]*groupings*, such that, given any two valid [7]*groupings*, there is a valid [11]*unique join grouping* that is [12]*the supremum (least upper bound) of* the two valid [7]*groupings*; and

c) There exists a [13]*meet function* in the set of [7]*groupings*, such that, given any two valid [7]*groupings*, there is a valid [14]*unique meet grouping* that is [12]*the infimum (greatest lower bound) of* the two valid [7]*groupings*.

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.

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 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 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 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.

6.1.9 FDP_ITT.1X Simple internal transfer protection

Hierarchical to: No other components.

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

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	access control SFP(s) and/or information flow control SFP(s)	*MDM grouping SFP*
[2]	selection	disclosure, modification, loss of use	*disclosure and modification*
[3]	refinement	separate parts of the TOE	*device attendants and manager attendants*

FDP_ITT.1X.1 The TSF shall enforce the [1]*MDM grouping SFP* to prevent the [2]*disclosure and modification* of user data when it is transmitted between [3]*device attendants and manager attendants*.

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.

6.1.10 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	allocation of the resource to, deallocation of the resource from	*deallocation of the resource from*
[2]	assignment	list of objects	*any buffer object that is used during the initiation or execution of a mobile device management function according to the MDM grouping SFP*

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [1]*deallocation of the resource from* the following objects: [2]*any buffer object that is used during the initiation or execution of a mobile device management function according to the MDM grouping SFP*.

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.

6.1.11 FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	all user data, the following user data [2]	*the following user data:* [2],
[2]	assignment	list of user data	*special categories of user data*
[3]	selection	temporary memory, persistent memory, any memory	*persistent memory*
[4]	refinement	[3]	[3] *controlled by the TSF*

FDP_SDC.1.1 The TSF shall ensure the confidentiality of [1]*the following user data:* [2]*special categories of user data,* while it is stored in the [3]*persistent memory* [4]*controlled by the TSF*.

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.

6.1.12 FDP_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	user data	*special categories of user data*
[2]	refinement	containers	*persistent memory*

FDP_SDI.1.1 The TSF shall monitor [1]*special categories of user data* stored in [2]*persistent memory* controlled by the TSF for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].

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.

6.1.13 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

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

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	access control SFP(s) and/or information flow control SFP(s)	*MDM grouping SFP*
[2]	selection	transmit, receive	*transmit and receive*

FDP_UCT.1.1 The TSF shall enforce the [1]*MDM grouping SFP* to [2]*transmit and receive* user data in a manner protected from unauthorised disclosure.

6.1.14 FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

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

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	access control SFP(s) and/or information flow control SFP(s)	*MDM grouping SFP*
[2]	selection	transmit, receive	*transmit and receive*
[3]	selection	modification, deletion, insertion, replay	*modification*

FDP_UIT.1.1 The TSF shall enforce the [1]*MDM grouping SFP* to [2]*transmit and receive* user data in a manner protected from [3]*modification* errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [3]*modification* has occurred.

6.1.15 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	list of security attributes	• *staff agent security attributes: role, cluster of groupings;* • *device agent security attributes: grouping*

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [1]

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

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	Refinement	TSF	*TOE device server security functionality*
[2]	Refinement	user	*device agent*

[DA]FIA_UAU.1.1 The [1]*TOE device server security functionality* shall allow [assignment: list of TSF mediated actions] on behalf of the [2]*device agent* to be performed before the [2]*device agent* is authenticated.

[DA]FIA_UAU.1.2 The [1]*TOE device server security functionality* shall require each [2]*device agent* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that [2]*device agent*.

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	TSF	*TOE control server security functionality*
[2]	refinement	user	*staff agent*

[SA]FIA_UAU.1.1 The [1]*TOE control server security functionality* shall allow [assignment: list of TSF mediated actions] on behalf of the [2]*staff agent* to be performed before the [2]*staff agent* is authenticated.

[SA]FIA_UAU.1.2 The [1]*TOE control server security functionality* shall require each [2]*staff agent* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that [2]*staff agent*.

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

Hierarchical to: No other components.

Dependencies: No dependencies

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	TSF	*TOE device server security functionality*
[2]	refinement	user	*device agent*

[DA]FIA_UID.1.1 The [1]*TOE device server security functionality* shall allow [assignment: list of TSF mediated actions] on behalf of the [2]*device agent* to be performed before the [2]*device agent* is identified.

[DA]FIA_UID.1.2 The [1]*TOE device server security functionality* shall require each [2]*device agent* to be successfully identified before allowing any other TSF-mediated actions on behalf of that [2]*device agent*.

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

Hierarchical to: No other components.

Dependencies: No dependencies

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	TSF	*TOE control server security functionality*
[2]	refinement	user	*staff agent*

[SA]FIA_UID.1.1 The [1]*TOE control server security functionality* shall allow [assignment: list of TSF mediated actions] on behalf of the [2]*staff agent* to be performed before the [2]*staff agent* is identified.

[SA]FIA_UID.1.2 The [1]*TOE control server security functionality* shall require each [2]*staff agent* to be successfully identified before allowing any other TSF-mediated actions on behalf of that [2]*staff agent*.

6.1.20 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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).

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	list of user security attributes	• *staff agent security attributes: role, cluster of groupings;* • *device agent security attributes: grouping*
[2]	assignment	rules for the initial association of attributes	• *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.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [1]

- *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: [2]

- *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: [assignment: rules for the changing of attributes].

6.1.21 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	determine the behaviour of, disable, enable, modify the behaviour of	*determine the behaviour of, disable, enable, and modify the behaviour of*
[2]	refinement (editorial)	functions [3]	[3]
[3]	assignment	list of functions	*device life-cycle management*
[4]	assignment	the authorised identified roles	*the administrator role*

FMT_MOF.1.1 The TSF shall restrict the ability to [1]*determine the behaviour of, disable, enable, and modify the behaviour of* the [2][3]*device life-cycle management* to [4]*the administrator role*.

6.1.22 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

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

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	access control SFP(s), information flow control SFP(s)	*MDM grouping SFP*
[2]	selection	change_default, query, modify, delete, [assignment: other operations]	*change_default, query, modify or delete*
[3]	refinement	security attributes	*information security attributes*
[4]	assignment	list of security attributes	*cluster of groupings*
[5]	assignment	the authorised identified roles	*the manager role*

FMT_MSA.1.1 The TSF shall enforce the [1]*MDM grouping SFP* to restrict the ability to [2]*change_default, query, modify or delete* the [3]*information security attributes* [4]*cluster of groupings* to [5]*the manager role*.

6.1.23 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	access control SFP(s), information flow control SFP(s)	*MDM grouping SFP*
[2]	selection (only one)	restrictive, permissive, [assignment: other property]	*permissive*
[3]	assignment	the authorised identified roles	*the manager role*
[4]	refinement	an object or information	*information*

FMT_MSA.3.1 The TSF shall enforce the [1]*MDM grouping SFP* to provide [2]*permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [3]*the manager role* to specify alternative initial values to override the default values when [4]*information* is created.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) Minimal: Use of the management functions.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	performing the following management functions	performing the following management functions *on behalf of a staff agent that is associated with the administrator role*
[2]	assignment	list of management functions to be provided by the TSF	• *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*

[AD]FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [1]*on behalf of a staff agent that is associated with the administrator role*: [2]

- *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*.

Application Note ([AD]FMT_SMF.1 – 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.

Application Note ([AD]FMT_SMF.1 – 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) Minimal: Use of the management functions.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	performing the following management functions	performing the following management functions *on behalf of a staff agent that is associated with the auditor role*
[2]	assignment	list of management functions to be provided by the TSF	• *review audit information*

[AU]FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [1]*on behalf of a staff agent that is associated with the auditor role*: [2]

- *review audit information*.

Application Note ([AU]FMT_SMF.1 – 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) Minimal: Use of the management functions.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement	performing the following management functions	performing the following management functions *on behalf of a staff agent that is associated with the manager role*
[2]	assignment	list of management functions to be provided by the TSF	• *review audit information;* • *change_default, query, modify or delete the information security attributes of the MDM grouping SFP*

[MA]FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [1]*on behalf of a staff agent that is associated with the manager role*: [2]

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

6.1.27 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	the authorised identified roles	*administrator, auditor, and manager*
[2]	refinement	be able to associate users with roles	*associate staff agents with roles*

FMT_SMR.1.1 The TSF shall maintain the roles [1]*administrator, auditor, and manager*.

FMT_SMR.1.2 The TSF shall [2]*associate staff agents with roles*.

6.1.28 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	disclosure, modification	*disclosure and modification*

FPT_ITT.1.1 The TSF shall protect TSF data from [1]*disclosure and modification* when it is transmitted between separate parts of the TOE.

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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	remote, local	*remote*
[2]	refinement	users	*device agents*
[3]	selection	modification, disclosure, [assignment: other types of integrity or confidentiality violation]	*modification and disclosure*
[4]	selection	the TSF, local users, remote users	*remote users*
[5]	selection	initial user authentication, [6]	[6]
[6]	assignment	other services for which trusted path is required	*device enrolment services*

[EN]FTP_TRP.1.1 The TSF shall provide a communication path between itself and [1]*remote* [2]*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 [3]*modification and disclosure*.

[EN]FTP_TRP.1.2 The TSF shall permit [4]*remote* [2]*device agents* to initiate communication via the trusted path.

[EN]FTP_TRP.1.3 The TSF shall require the use of the trusted path for [5][6]*device enrolment services*.

Application Note ([EN]FTP_TRP.1). 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	remote, local	*remote*
[2]	refinement	users	*authorised device agents*
[3]	selection	modification, disclosure [assignment: other types of integrity or confidentiality violation]	*modification and disclosure*
[4]	selection	the TSF, local users, remote users	*remote users*
[5]	selection	initial user authentication, [6]	*initial user authentication, and* [6]
[6]	assignment	other services for which trusted path is required	*mobile device management*

[DA]FTP_TRP.1.1 The TSF shall provide a communication path between itself and [1]*remote* [2]*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 [3]*modification and disclosure*.

[DA]FTP_TRP.1.2 The TSF shall permit [4]*remote* [2]*authorised device agents* to initiate communication via the trusted path.

[DA]FTP_TRP.1.3 The TSF shall require the use of the trusted path for [5]*initial user authentication, and* [6]*mobile device management*.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	selection	remote, local	*remote*
[2]	refinement	users	*authorised staff agents*
[3]	selection	modification, disclosure [assignment: other types of integrity or confidentiality violation]	*modification and disclosure*
[4]	selection	the TSF, local users, remote users	*remote users*
[5]	selection	initial user authentication, [6]	*initial user authentication, and* [6]
[6]	assignment	other services for which trusted path is required	*all services provided to authorised staff agents*

[SA]FTP_TRP.1.1 The TSF shall provide a communication path between itself and [1]*remote* [2]*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 [3]*modification and disclosure*.

[SA]FTP_TRP.1.2 The TSF shall permit [4]*remote* [2]*authorised staff agents* to initiate communication via the trusted path.

[SA]FTP_TRP.1.3 The TSF shall require the use of the trusted path for [5]*initial user authentication, and* [6]*all services provided to authorised staff agents*.

6.2 Security Assurance Requirements (SARs)

The SAR components are taken from CC Part 3 and referenced in Table 6. They correspond to package EAL4 augmented with 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

Table 6: Security Assurance Requirements (SARs)

6.3 Security Requirements Rationale

6.3.1 Justification of SFR/SAR dependencies

All dependencies of the SAR components are satisfied.

All dependencies of the SFR components are satisfied, not applicable (void) or addressed by security objectives for the operational environment (see Table 7).

SFR component	*Dependencies*	*Justification*
FAU_GEN.1	FPT_STM.1	OE.ReliableTimestamps
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.3	FAU_STG.1	OE.AuditTrail
FDP_IFC.1	FDP_IFF.1	satisfied by FDP_IFF.2 (hierarchical)
FDP_IFF.2	FDP_IFC.1	satisfied
	FMT_MSA.3	satisfied
FDP_ITT.1X	FDP_ACC.1 or FDP_IFC.1	void satisfied
FDP_RIP.1	—	—
FDP_SDC.1	—	—
FDP_SDI.1	—	—
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1	void satisfied [iterations for device/staff agents]
	FDP_ACC.1 or FDP_IFC.1	void satisfied
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1	void satisfied
	FTP_ITC.1 or FTP_TRP.1	void satisfied [iterations for device/staff agents]
FIA_ATD.1	—	—
[DA]FIA_UAU.1	FIA_UID.1	satisfied [iteration for device agents]
[SA]FIA_UAU.1	FIA_UID.1	satisfied [iteration for staff agents]
[DA]FIA_UID.1	—	—
[SA]FIA_UID.1	—	—
FIA_USB.1	FIA_ATD.1	satisfied
FMT_MOF.1	FMT_SMR.1	satisfied
	FMT_SMF.1	satisfied [iteration for administrator agents]

FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	void satisfied
	FMT_SMR.1	satisfied
	FMT_SMF.1	satisfied [iteration for manager agents]
FMT_MSA.3	FMT_MSA.1	satisfied
	FMT_SMR.1	satisfied
[AD]FMT_SMF.1	—	—
[AU]FMT_SMF.1	—	—
[MA]FMT_SMF.1	—	—
FMT_SMR.1	FIA_UID.1	satisfied [iteration for staff agents]
FPT_ITT.1	—	—
[EN]FTP_TRP.1	—	—
[DA]FTP_TRP.1	—	—
[SA]FTP_TRP.1	—	—

Table 7: Justification of SFR dependencies

6.3.2 SFRs trace to and meet all security objectives for the TOE

All SFR components trace to security objectives for the TOE (see Table 8).

The objective OT.COMMUNICATION is met as follows:

Provision of mutually authenticated trusted communication paths as required by [SA]FTP_TRP.1 and [DA]FTP_TRP.1 prevents unauthorised disclosure and modification of data exchanged between parts of the TOE and remote authorised device/staff agents as external entities.

The objective OT.DEVICELIFECYCLE is met as follows:

The device enrolment services are protected by providing a trusted communication path as required by [EN]FTP_TRP.1. 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 [AD]FMT_SMF.1, FMT_MOF.1 and FMT_SMR.1. The authorisation of administrator agents is required prior to any management action by [SA]FIA_UID.1 (staff agent identification), [SA]FIA_UAU.1 (staff agent authentication) and FIA_ATD.1 (definition of attribute role).

Tracing of SFR components to security objectives for the TOE	OT.COMMUNICATION	OT.DEVICELIFECYCLE	OT.DEVICETRACKING	OT.LOGGING	OT.MANAGEMENT	OT.SEPARATION	OT.STORAGE
FAU_GEN.1			×	×			
FAU_GEN.2			×	×			
FAU_SAR.1			×	×			
FAU_SAR.2			×	×			
FAU_SAR.3			×				
FAU_STG.3			×	×			
FDP_IFC.1					×		
FDP_IFF.2					×		
FDP_ITT.1X					×		
FDP_RIP.1							×
FDP_SDC.1							×
FDP_SDI.1							×
FDP_UCT.1						×	
FDP_UIT.1						×	
FIA_ATD.1		×	×	×	×	×	
[DA]FIA_UAU.1			×		×	×	
[SA]FIA_UAU.1		×	×	×	×	×	
[DA]FIA_UID.1			×		×	×	
[SA]FIA_UID.1		×	×	×	×	×	
FIA_USB.1					×	×	
FMT_MOF.1		×					
FMT_MSA.1					×		
FMT_MSA.3					×		
[AD]FMT_SMF.1		×					
[AU]FMT_SMF.1			×	×			
[MA]FMT_SMF.1			×		×		
FMT_SMR.1		×	×	×	×		
FPT_ITT.1					×		
[EN]FTP_TRP.1		×					
[DA]FTP_TRP.1	×					×	
[SA]FTP_TRP.1	×					×	

Table 8: Tracing of SFR components to security objectives for the TOE

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.3 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. [DA]FIA_UAU.1 and [DA]FIA_UID.1 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, [AU]FMT_SMF.1 and [MA]FMT_SMF.1 define the staff agents that are allowed to read audit information. FAU_SAR.1 and FAU_SAR.3 distinguish 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. [SA]FIA_UAU.1 and [SA]FIA_UID.1 make sure that staff agents are successfully identified and authenticated before they gain read access to audit information.

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.3 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. [SA]FIA_UAU.1 and [SA]FIA_UID.1 make sure that staff agents are successfully identified and authenticated.

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 ([SA]FIA_UAU.1 and [SA]FIA_UID.1) and device agents ([DA]FIA_UAU.1 and [DA]FIA_UID.1) 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 5. 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 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.

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. [SA]FIA_UID.1 and [SA]FIA_UAU.1 guarantee that manager agents are identified and authenticated before they can communicate with the manager attendant. Similarly, [DA]FIA_UID.1 and [DA]FIA_UAU.1 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 ([SA]FTP_TRP.1) and device agents ([DA]FTP_TRP.1).

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.

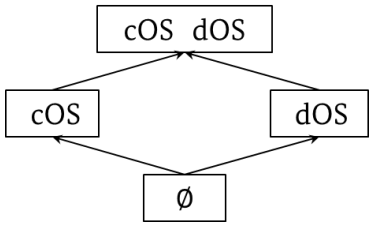
6.3.3 Explanation of the chosen SARs

The chosen SAR package EAL4 provides a consistent level of rigour and assurance that is appropriate to the type of the TOE. For security flaws detected in the TOE once evaluated and certified, the TOE developer is expected to have systematic flaw remediation procedures in place, therefore ALC_FLR.3 is augmented.

7 Appendix: Bounded Lattice of Groupings

7.1 A simple bounded lattice of groupings

Imagine a fictitious company running an MDM system that manages a certain number of mobile devices. Let us assume that devices with two different operating systems, say cloneOS (cOS) and droneOS (dOS), are managed, and that there is a manager responsible for cloneOS devices and a manager responsible for droneOS devices.



In this case a simple bounded lattice as depicted in the diagram above would suffice. Each device is given the grouping attribute that matches its operating system; likewise, each of the two managers according to their responsibilities.

A formal definition of this simple bounded lattice is possible in two ways.

- By explicitly naming the elements of the lattice, the partial ordering (with unique maximum and minimum elements), and the join and meet functions as follows:

  Let OS be the set of operating systems: $OS = \{\text{cOS,dOS}\}$

  As the lattice elements take the set OSs of all subsets of OS:
  $OSs = \{\emptyset, \{\text{cOS}\}, \{\text{dOS}\}, \{\text{cOS,dOS}\}\}$

  Partial ordering: For any two lattice elements $P, Q \in OSs$:
  $P \leq Q$ if and only if $P = Q$ or there exists a path from P to Q in the diagram above

  Join function $\sqcup$ is commutative and idempotent, and for any lattice element $P \in OSs$:
  $\emptyset \sqcup P = P$, $\{\text{cOS,dOS}\} \sqcup P = \{\text{cOS,dOS}\}$, $\{\text{cOS}\} \sqcup \{\text{dOS}\} = \{\text{cOS,dOS}\}$

  Meet function $\sqcap$ is commutative and idempotent, and for any lattice element $P \in OSs$:
  $\emptyset \sqcap P = \emptyset$, $\{\text{cOS,dOS}\} \sqcap P = P$, $\{\text{cOS}\} \sqcap \{\text{dOS}\} = \emptyset$

  Note that the definition of a bounded lattice in this way might be error prone. In general, it is necessary to demonstrate that the join and meet functions indeed result in the supremum and infimum respectively.

- By using basic operations from set theory:

  Let OS be the set of operating systems: $OS = \{\text{cOS,dOS}\}$

  Lattice elements: $OSs = \{S \mid S \subseteq OS\}$ (the set of all subsets of OS)

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

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

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

  It is well known that this powerset construction over a finite set results in a bounded lattice.

7.2 A straightforward bounded lattice of tenant groupings

Suppose the MDM Trusted Server provides multi-tenancy support. Each device would be assigned to a single tenant whereas each manager would be assigned to several tenants.

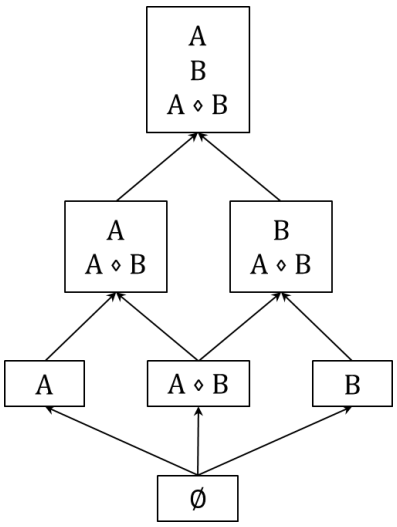
Let us assume that there is a number of n different tenants $\mathrm{Tenant}_1, \ldots, \mathrm{Tenant}_n$. Then the bounded lattice might be formally defined using the powerset construction as in the previous example.

Let $Tenants$ be the set of all tenants: $Tenants = \{\mathrm{Tenant}_1, \ldots, \mathrm{Tenant}_n\}$

Lattice elements:	$Ts = \{T \mid T \subseteq Tenants\}$	(the set of all subsets of $Tenants$)
Partial ordering:	$\forall U, V \in Ts\colon\ U \leq V \equiv U \subseteq V$	(subset relation)
Join function:	$\forall U, V \in Ts\colon\ U \sqcup V = U \cup V$	(set union)
Meet function:	$\forall U, V \in Ts\colon\ U \sqcap V = U \cap V$	(set intersection)

7.3 A more intricate bounded lattice of groupings

Suppose the fictitious company is distributed across two locations, say Athens (A) and Berlin (B). Some employees work exclusively in Athens, others work exclusively in Berlin, and some work at both locations. An appropriate bounded lattice of groupings would look as depicted in the diagram below.



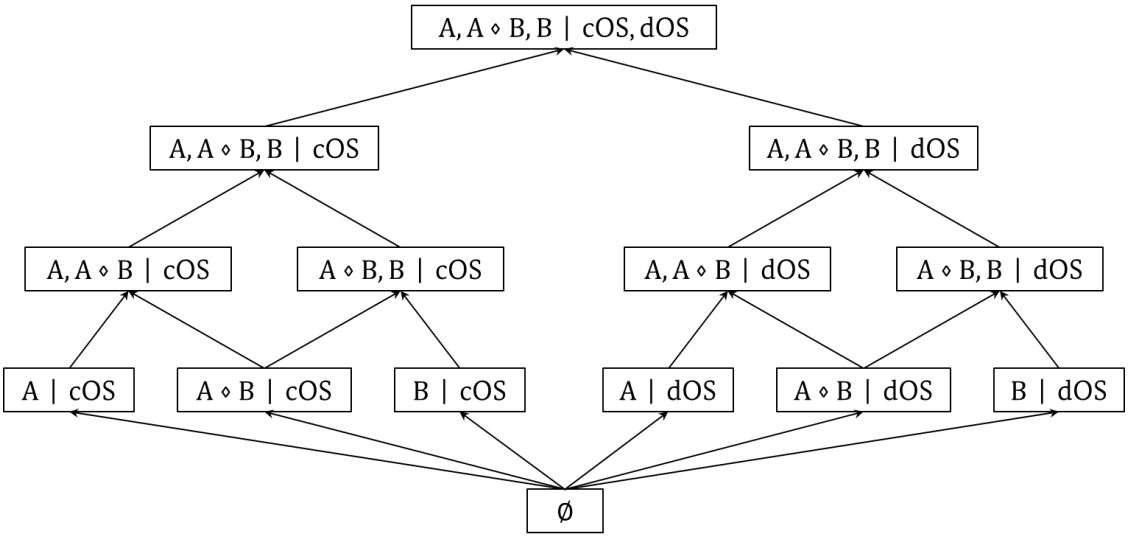
Each device would receive a grouping from the third row and each manager would receive a grouping from the first or second row. This guarantees that a manager responsible for all the devices in Athens can issue commands not only to those exclusively in Athens, but also to those which belong to both Athens and Berlin.

Devices belonging to both Athens and Berlin can be managed by every manager, but only a manager with the first grouping of the second row (or greater) can manage devices exclusively in Athens (and likewise for the devices exclusively in Berlin).

Please note that a formal definition of this more intricate bounded lattice is not possible using the power set construction because the subset {A,B} is not an element of the lattice. Therefore, the supremum of {A} and {B} is not {A,B} but {A,B,A ⋄ B}.

7.4 A combined bounded lattice of groupings

Let us consider the differentiations of location and operating system together. An appropriate bounded lattice of groupings for this case could be described as in the diagram below.



Each device would receive one of the groupings in the fourth row, and staff agents would receive a cluster of groupings in one of the upper three rows.

For instance, according to FAU_SAR.3.1, a staff agent who is responsible for all cloneOS devices (first grouping, second row) can choose to review filtered audit data from cloneOS devices located in Athens (first grouping, fourth row), but not from droneOS devices located in Berlin (sixth grouping, fourth row) because the infimum of the two groupings is the bottom grouping.

Similarly, according to FDP_IFF.2.2, a manager attendant who may issue commands to droneOS devices located in Athens (third grouping, third row) is not allowed to send a 'remote lock' to a cloneOS device located in Athens (first grouping, fourth row), but may do so for a droneOS device located in both Athens and Berlin (fifth grouping, fourth row).

Clustering of groupings introduce more flexibility in the handling of management responsibilities. For instance, a manager attendant may be given a cluster of two groupings for Athens (first and third grouping, third row). This way, the manager attendant can manage each device that is located in Athens, regardless of its operating systems.

Note that, unless there is a top manager with the maximum grouping, the MDM administration should make sure that the manager grouping attributes are properly distributed. For instance, if there is a manager responsible for all cloneOS devices regardless of the location (first grouping of the second row) and another manager responsible for droneOS devices located in Athens (third grouping of the third row), the lattice reveals that nobody could possibly issue management commands to droneOS devices located in Berlin (sixth grouping of the fourth row). Thus, the hierarchical structure of grouping attributes in form of a lattice supports avoiding management gaps.

7.5 A systematic combination of bounded sub-lattices

Finally, let us combine two exemplary bounded sub-lattices to a combined bounded lattice. We consider an MDM Trusted Server that is able to manage mobile devices of several tenants, but also distinguishes between locations and operating systems of mobile devices.

Let the bounded sub-lattices on the set Ts of tenant groupings as defined in section 7.2 and on the set Os of locations and operating systems as defined in section 7.4. Then we define the combined bounded lattice component-by-component on ordered pairs:

Lattice elements:	$\{(T, O) \mid T \in Ts, O \in Os\}$
Partial ordering:	$(T_1, O_1) \leq (T_2, O_2) \equiv T_1 \leq T_2 \wedge O_1 \leq O_2$
Join function:	$(T_1, O_1) \sqcup (T_2, O_2) = (T_1 \sqcup T_2, O_1 \sqcup O_2)$
Meet function:	$(T_1, O_1) \sqcap (T_2, O_2) = (T_1 \sqcap T_2, O_1 \sqcap O_2)$

Please note that the symbols for the join function, the meet function and the partial ordering relation are overloaded in the above definition.

The combination of locations and operating systems given section 7.4 differs from the systematic combination of bounded sub-lattices, because the set Os is not identical to the set of ordered pairs of locations and operating systems. Among others, the pairs $(\{\mathrm{A}\}, \emptyset)$ and $(\{B\}, \{\mathrm{cOS,dOS}\})$ are missing in Os.

The construction of bounded lattices from given bounded sub-lattices can easily be generalised to a combination of an arbitrary number of bounded sub-lattices by defining the combined bounded lattice component-by-component on n-tuples of elements from the respective bounded sub-lattices.