Federal Office
for Information Security

PP-Configuration Mobile Device Management – Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC)

Common Criteria Protection Profile Configuration
BSI-CC-PP-0116, 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

PP-Configuration Reference

Title	PP-Configuration Mobile Device Management – Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC)
Short title	PP-Configuration MDM-TS-TCC
Version	1.0
Registration	BSI-CC-PP-0116
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)

Components Statement

This PP-Configuration contains the following components:

- PP Mobile Device Management – Trusted Server (MDM-TS), BSI-CC-PP-0115, Version 1.0
- PP-Module Trusted Communication Channel (TCC), PPM-TCC, Version 1.0

Conformance Statement

This PP-Configuration claims conformance to Common Criteria Version 3.1 Revision 5 (CC 3.1 R5).

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

SAR Statement

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

– End of PP-Configuration –

Federal Office
for Information Security

PP-Module
Trusted Communication Channel (TCC)

Common Criteria Protection Profile Module
PP-Module TCC, Version 1.0

Change history

Version	*Date*	*Description*
1.0	27.09.2021	Approved edition for initial release for combination with Base-PP MDM-TS (BSI-CC-PP-0115)

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 tables

1 PP-Module Introduction

1.1 PP-Module Reference

Title	PP-Module Trusted Communication Channel (TCC)
Short title	PP-Module TCC
Version	1.0
Registration	as component of the following PP-Configuration(s): BSI-CC-PP-0116
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 Base-PP Identification

This PP-Module relies on the following Base-PP:

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

1.3 TOE Overview

The scope of this PP-Module is to describe the security functionality of trusted communication channels which complement the security functionality stated by the PP Mobile Device Management – Trusted Server (MDM-TS).

The TOE type remains as described in PP MDM-TS.

The usage and major security features of the TOE generally remain as described in PP MDM-TS.

This PP-Module introduces additional major security features of the TOE for establishing and using trusted communication channels which protect user and TSF data in transit between external entities and the TOE.

The TOE does not rely on non-TOE hardware/software but provides trusted communication channels by itself. Other necessary non-TOE hardware/software remains as described in PP MDM-TS.

2 Conformance Claims

2.1 CC Conformance Claim

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

- CC Part 2 extended with component FCS_CKM.5 and family FTP_PRO

2.2 Package Claim

This PP-Module does not claim conformance to any security functional requirements package.

3 Security Problem Definition

3.1 Threats

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.

3.2 Organisational Security Policies

This PP-Module does not define any organisational security policies.

3.3 Assumptions

This PP-Module does not define any assumptions about the operational environment of the TOE.

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. The protection of confidentiality and integrity shall be based on the use of trusted communication channels.

OT.TRUSTEDCOMMUNICATIONCHANNEL

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

4.2 Security Objectives for the Operational Environment

This PP-Module does not define any security objectives for the operational environment of the TOE.

4.3 Security Objectives Rationale

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

Tracing of security objectives to threats	T.COMPROMISED-COMMUNICATION
OT.COMMUNICATION	×
OT.TRUSTEDCOMMUNICATIONCHANNEL	×

Table 1: Tracing of security objectives to threats

The threat T.COMPROMISEDCOMMUNICATION is countered by the objective OT.COMMUNICATION which is supported by the objective OT.TRUSTEDCOMMUNICATIONCHANNEL, as these security 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.

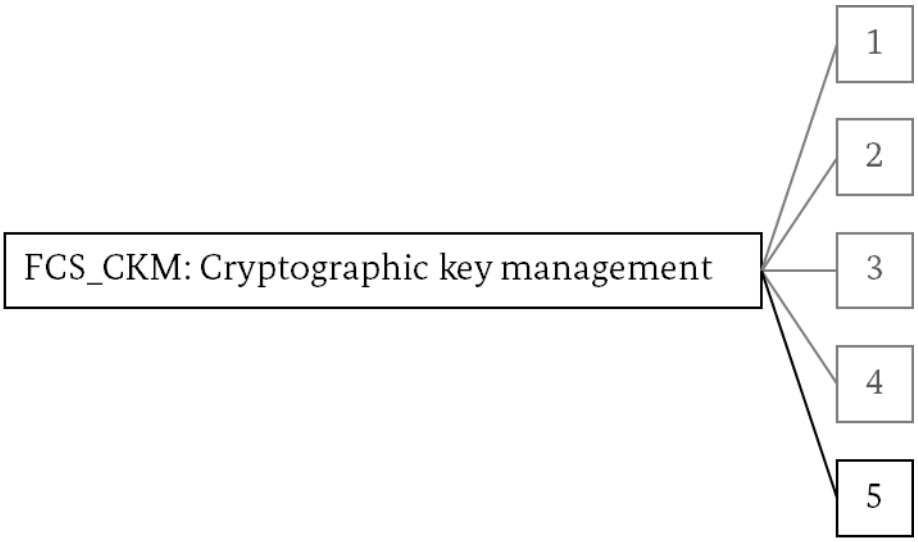
5 Extended Components Definition

5.1 Cryptographic Key Management (FCS_CKM)

Family behaviour

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access, cryptographic key destruction and cryptographic key derivation. This family should be included whenever there are functional requirements for the management of cryptographic keys.

Component levelling



The components FCS_CKM.1/.2/.3/.4 are already defined (see CC Part 2, Par. 143-146).

FCS_CKM.5 *Cryptographic key derivation*, describes functional requirements for key derivation as process by which one or more keys are calculated from either a pre-shared key or a shared secret and other information.

Management: FCS_CKM.5

There are no management activities foreseen.

Audit: FCS_CKM.5

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: Success and failure of the activity.

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

FCS_CKM.5 Cryptographic key derivation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys [assignment: key type] from [assignment: input parameters] in accordance with a specified cryptographic key derivation algorithm [assignment: cryptographic key derivation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

5.2 Trusted Channel Protocol (FTP_PRO)

Family behaviour

This family defines requirements for establishing a trusted channel and using the trusted channel to transfer the TSF data or user data securely.

Component levelling

FTP_PRO.1 *Trusted channel protocol* requires that communication be established in accordance with a defined protocol.

FTP_PRO.2 *Trusted channel establishment* requires that keys be securely established between the peers.

FTP_PRO.3 *Trusted channel data protection* requires that data in transit be protected.

Management: FTP_PRO.1

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

a) Configuring the protocols needed for the trusted channel;
b) Configuring the credentials for using the trusted channel;
c) Configuring the conditions for initialising and terminating the trusted channel.

Management: FTP_PRO.2

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

a) Configuring the parameters for shared secrets;

b) Configuring the parameters for cryptographic key derivation.

Management: FTP_PRO.3

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

a) Configuring the encryption and integrity mechanisms used by the trusted channel.

Audit: FTP_PRO.1

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: Failure of the trusted channel establishment.

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

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

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

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

Audit: FTP_PRO.2

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: Authentication failures during channel establishment.

b) Basic: All authentication attempts.

Audit: FTP_PRO.3

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

FTP_PRO.1 Trusted channel protocol

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 Trusted channel establishment
FTP_PRO.3 Trusted channel data protection.

FTP_PRO.1.1 **The TSF shall implement [assignment: trusted channel protocol] acting as [assignment: defined protocol role(s)] in accordance with: [assignment: list of standards].**

FTP_PRO.1.2 **The TSF shall enforce usage of the trusted channel for [assignment: purpose(s) of the trusted channel] in accordance with: [assignment: list of standards].**

FTP_PRO.1.3 The TSF shall permit [selection: itself, its peer] to initiate communication via the trusted channel.

FTP_PRO.1.4 The TSF shall enforce the following rules for the trusted channel: [assignment: rules governing operation and use of the trusted channel and/or its protocol].

FTP_PRO.1.5 The TSF shall enforce the following static protocol options: [assignment: list of options and references to standards in which each is defined].

FTP_PRO.1.6 The TSF shall negotiate one of the following protocol configurations with its peer: [assignment: list of configurations and reference to standards in which each is defined].

FTP_PRO.2 Trusted channel establishment

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 Trusted channel protocol
[FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.2 Cryptographic key distribution]
FCS_CKM.5 Cryptographic key derivation
FCS_COP.1 Cryptographic operation.

FTP_PRO.2.1 The TSF shall establish a shared secret with its peer using one of the following mechanisms: [assignment: list of key establishment mechanisms].

FTP_PRO.2.2 The TSF shall authenticate [selection: its peer, itself to its peer] using one of the following mechanisms: [assignment: list of authentication mechanisms] and according to the following rules: [assignment: list of rules for carrying out the authentication].

FTP_PRO.2.3 The TSF shall use [assignment: key derivation function] to derive the following cryptographic keys from a shared secret: [assignment: list of cryptographic keys].

FTP_PRO.3 Trusted channel data protection

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 Trusted channel protocol
FTP_PRO.2 Trusted channel establishment
FCS_COP.1 Cryptographic operation.

FTP_PRO.3.1 The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [assignment: list of encryption mechanisms].

FTP_PRO.3.2 The TSF shall protect data in transit from [selection: modification, deletion, insertion, replay, [assignment: other]] using one of the following mechanisms: [assignment: list of integrity protection mechanisms].

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.

6.1.1 FCS_CKM.5 Cryptographic key derivation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
	FCS_CKM.4 Cryptographic key destruction

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

a) Minimal: Success and failure of the activity.

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

FCS_CKM.5.1 **The TSF shall derive cryptographic keys [assignment: key type] from [assignment: input parameters] in accordance with a specified cryptographic key derivation algorithm [assignment: cryptographic key derivation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].**

Application notes (FCS_CKM.5).

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

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

6.1.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

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

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

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

FCS_COP.1.1 **The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].**

Application notes (FCS_COP.1).

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

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

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

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

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

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

In each iteration of FCS_COP.1 in the PP/ST, in the assignment about the ‘list of cryptographic operations’ the PP/ST author should also identify the corresponding keys being used. This will allow to easily map the FCS_COP.1 iterations to the related dependencies and security objectives, respectively.

Finally, for all iterations of FCS_COP.1 the choice of cryptographic algorithms and cryptographic key sizes should ensure the minimum security level of 100 bit for all cryptographic operations in their corresponding use case or protocol. The PP/ST author should follow the recommendations of the latest edition of the BSI Technical Guideline TR-02102[1] on cryptographic mechanisms when choosing cryptographic primitives, protocols, and parameters. Depending on the certification scheme, other recommendations for the choice of cryptographic mechanisms, such as the SOG-IS Agreed Cryptographic Mechanisms[2], may also be considered.

6.1.3 FTP_PRO.1 Trusted channel protocol

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 Trusted channel establishment
FTP_PRO.3 Trusted channel data protection.

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

a) Minimal: Failure of the trusted channel establishment.
b) Minimal: Identification of the initiator and target of failed trusted channel establishment.
c) Basic: All attempted uses of the trusted channel.
d) Basic: Identification of the initiator and target of all trusted channel attempts.

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

FTP_PRO.1.1 **The TSF shall implement [assignment: trusted channel protocol] acting as [assignment: defined protocol role(s)] in accordance with: [assignment: list of standards].**

FTP_PRO.1.2 **The TSF shall enforce usage of the trusted channel for [assignment: purpose(s) of the trusted channel] in accordance with: [assignment: list of standards].**

FTP_PRO.1.3 **The TSF shall permit [selection: itself, its peer] to initiate communication via the trusted channel.**

FTP_PRO.1.4 **The TSF shall enforce the following rules for the trusted channel: [assignment: rules governing operation and use of the trusted channel and/or its protocol].**

FTP_PRO.1.5 **The TSF shall enforce the following static protocol options: [assignment: list of options and references to standards in which each is defined].**

FTP_PRO.1.6 **The TSF shall negotiate one of the following protocol configurations with its peer: [assignment: list of configurations and reference to standards in which each is defined].**

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

---

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

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

6.1.4 FTP_PRO.2 Trusted channel establishment

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 Trusted channel protocol
[FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.2 Cryptographic key distribution]
FCS_CKM.5 Cryptographic key derivation
FCS_COP.1 Cryptographic operation.

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

a) Minimal: Authentication failures during channel establishment.

b) Basic: All authentication attempts.

FTP_PRO.2.1 **The TSF shall establish a shared secret with its peer using one of the following mechanisms: [assignment: list of key establishment mechanisms].**

FTP_PRO.2.2 **The TSF shall authenticate [selection: its peer, itself to its peer] using one of the following mechanisms: [assignment: list of authentication mechanisms] and according to the following rules: [assignment: list of rules for carrying out the authentication].**

FTP_PRO.2.3 **The TSF shall use [assignment: key derivation function] to derive the following cryptographic keys from a shared secret: [assignment: list of cryptographic keys].**

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

6.1.5 FTP_PRO.3 Trusted channel data protection

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 Trusted channel protocol
FTP_PRO.2 Trusted channel establishment
FCS_COP.1 Cryptographic operation.

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

[1]	selection	modification, deletion, insertion, replay, [assignment: other]	*modification*

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

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

FTP_PRO.3.1 **The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [assignment: list of encryption mechanisms].**

FTP_PRO.3.2 **The TSF shall protect data in transit from [1]*modification* using one of the following mechanisms: [assignment: list of integrity protection mechanisms].**

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

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

This SFR component is inherited from the PP MDM-TS.

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

This SFR component is inherited from the PP MDM-TS.

6.2 Security Requirements Rationale

6.2.1 Justification of SFR dependencies

All dependencies of the SFR components are satisfied, or to be addressed by the PP/ST author (see Table 2).

SFR component	*Dependencies*	*Justification*
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	to be addressed by the PP/ST author to be addressed by the PP/ST author to be addressed by the PP/ST author
	FCS_CKM.4	to be addressed by the PP/ST author
FCS_CKM.5	FCS_CKM.2 or FCS_COP.1	to be addressed by the PP/ST author to be addressed by the PP/ST author
	FCS_CKM.4	to be addressed by the PP/ST author
FTP_PRO.1	FTP_PRO.2	satisfied
	FTP_PRO.3	satisfied
FTP_PRO.2	FTP_PRO.1	satisfied
	FCS_CKM.1 or FCS_CKM.2	to be addressed by the PP/ST author to be addressed by the PP/ST author
	FCS_CKM.5	satisfied
	FCS_COP.1	satisfied
FTP_PRO.3	FTP_PRO.1	satisfied
	FTP_PRO.2	satisfied
	FCS_COP.1	satisfied
[DA]FTP_TRP.1	—	—
[SA]FTP_TRP.1	—	—

Table 2: Justification of SFR dependencies

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

All SFR components trace to security objectives for the TOE (see Table 3).

Tracing of SFR components to security objectives for the TOE	OT.COMMUNICATION	OT.TRUSTED-COMMUNICATIONCHANNEL
FCS_CKM.5		×
FCS_COP.1		×
FTP_PRO.1		×
FTP_PRO.2		×
FTP_PRO.3	×	×
[DA]FTP_TRP.1	×	
[SA]FTP_TRP.1	×	

Table 3: Tracing of SFR components to security objectives for the TOE

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 staff/device agents as external entities.

FTP_PRO.3 ensures that the protection of confidentiality and integrity is based on the use of mutually authenticated trusted communication channels.

The objective **OT.TRUSTEDCOMMUNICATIONCHANNEL** is met as follows:

FTP_PRO.1, FTP_PRO.2 and FTP_PRO.3 provide mutually authenticated trusted communication channels by using trusted channel protocols based on cryptographic mechanisms.

FTP_PRO.1 ensures that communication be established in accordance with a defined protocol.

FTP_PRO.2 ensures that keys be securely established between the peers using appropriate cryptographic mechanisms (FCS_COP.1) and appropriate cryptographic key derivation (FCS_CKM.5).

FTP_PRO.3 ensures that data in transit be protected from unauthorised disclosure and modification using appropriate cryptographic operations (FCS_COP.1).

7 Consistency Rationale

7.1 Consistency of the TOE type

As this PP-Module is used to complement the PP MDM-TS, the TOE type for the overall TOE is still a *Mobile Device Management – Trusted Server (MDM-TS)*. Instead of relying on non-TOE hardware / software, the TOE boundary is extended to include the security functionality of trusted communication channels in order to ensure confidentiality and integrity of data in transit.

7.2 Consistency of the Security Problem Definition

The security problem defined by this PP-Module is consistent with the PP MDM-TS based on the following rationale.

T.CompromisedCommunication

> The PP MDM-TS contains this same threat with the same threat agent, assets and adverse actions.

7.3 Consistency of the Security Objectives

The security objectives described by this PP-Module are consistent with the PP MDM-TS based on the following rationale.

OT.Communication

> This security objective for the TOE results from the refinement of the corresponding security objective contained in the PP MDM-TS with the same purpose. It aims at extending the TOE boundary to include the security functionality of trusted communication channels.

OT.TrustedCommunicationChannel

> The MDM PP contains an equivalent security objective for the operational environment with the same purpose. It becomes a security objective for the TOE in this PP-Module.

7.4 Consistency of the Security Functional Requirements

The security functional requirements described by this PP-Module are consistent with the PP MDM-TS based on the following rationale.

[DA]FTP_TRP.1, [SA]FTP_TRP.1

> These security functional requirements come from the PP MDM-TS and are needed to meet the refined security objective OT.Communication.

FCS_CKM.5, FCS_COP.1, FTP_PRO.1, FTP_PRO.2, FTP_PRO.3

> These security functional requirements are new and introduce trusted communication channels to the TOE in order to meet the security objectives OT.TrustedCommunicationChannel and OT.Communication.