ETSI TS 103 732-5 V1.1.1 (2024-07)

Cyber Security (CYBER);
Consumer Mobile Device;
Part 5: Bootloader & Root of Trust Protection Profile Module

Reference
DTS/CYBER-00128

Keywords
cybersecurity, mobile, privacy, terminal

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 5 of a multi-part deliverable covering the Consumer Mobile Device, as identified below:

Part 1: "Base Protection Profile";

Part 2: "Biometric Authentication Protection Profile Module";

Part 3: "Multi-user Protection Profile Module";

Part 4: "Preloaded Applications Protection Profile Module";

Part 5: "Bootloader & Root of Trust Protection Profile Module".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines a PP-Module for Consumer Mobile Device (CMD) which adds additional security requirements focused on the bootloader and storage configuration.

The present document identifies key security requirements for how the bootloader should be configured to protect the integrity of the CMD.

The present document is intended for CMD manufacturers implementing those security requirements for device certification and for third parties looking to assess the security functions on CMD such as evaluators.

The Target Of Evaluation (TOE) described by the present document is the bootloader and the storage configuration included on a CMD.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] CCMB-2017-04-001 Version 3.1 revision 5, April 2017: "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model".

[2] CCMB-2017-04-002 Version 3.1 revision 5, April 2017: "Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components".

[3] CCMB-2017-04-003 Version 3.1 revision 5, April 2017: "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components".

[4] CCMB-2017-04-004 Version 3.1 revision 5, April 2017: "Common Methodology for Information Technology Security Evaluation - Evaluation methodology".

[5] CCDB-2017-05-xxx Version 0.5, May 2017: "CC and CEM addenda - Exact Conformance, Selection-Based SFRs, Optional SFRs".

[6] ETSI TS 103 732-1 (V2.1.2): "CYBER; Consumer Mobile Device; Part 1: Base Protection Profile".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

bootloader: program used to load the main OS (or alternative recovery systems or boot modes) into memory

consumer mobile device: user customizable device utilizing an operating system, supporting installation and maintenance of applications, with wireless internet connectivity, high computation power and rich user interface, used for various purposes by the individual owner

NOTE: As defined in ETSI TS 103 732-1 [6].

CPU privilege level: mode of operation within the CPU that establishes the level of permissions to system resources (such as memory or hardware interrupts)

locked bootloader: bootloader that has been configured to only load the main OS after the signature has been verified

main OS: primary operating system of the device (as opposed to subsystems that may provide specialized, usually security-related, functions)

NOTE: As defined in ETSI TS 103 732-1 [6].

Root of Trust (RoT): essential, foundational security component that provides a set of trustworthy functions that the rest of the device or system can use to establish strong levels of security

Security Assurance Requirement (SAR): description of how assurance is to be gained that the TOE meets the SFRs

NOTE: As defined in [1].

Security Functional Requirement (SFR): requirement, stated in a standardized language, which is meant to contribute to achieving the security objectives for a TOE

NOTE: As defined in [1].

security objective: statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

NOTE: As defined in [1].

security problem: statement, which in a formal manner defines the nature and scope of the security that the TOE is intended to address

NOTE: As defined in [1].

storage configuration: logical division of the storage system into separate areas used by the operating system

target of evaluation: set of software, firmware and/or hardware possibly accompanied by guidance

NOTE: As defined in [1].

TOE security functionality: combined functionality of all hardware, software, and firmware of a TOE that are relied upon for the correct enforcement of the security functional requirements

NOTE: As defined in [1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CC	Common Criteria
CMD	Consumer Mobile Device
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
ECD	Extended Component Definition
OS	Operating System
PP	Protection Profile
RoT	Root of Trust
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

4 TOE Definition

4.1 TOE Overview

The Base-PP [6] does not specify any requirements related to the bootloader, apart to run a suite of self tests on it to verify its integrity (see FPT_TST.1 TSF testing in ETSI TS 103 732-1 [6]), or the establishment of a Root of Trust of the CMD. A Root of Trust provides a way to ensure that the device has not been tampered with, and can be used to ensure secure computations are authentic on the device, including verifying the components being loaded into memory as trusted. The bootloader is critical for the security of the CMD as it is the first thing to be loaded and run when the CMD is powered on, building on the chain of trust based on the Root of Trust, to that eventually ends with the main OS being fully loaded.

This PP-Module introduces additional security requirements to the TOE as defined in ETSI TS 103 732-1 [6]. The additional requirements are related to the bootloader, the storage configuration and the Root of Trust on the CMD.

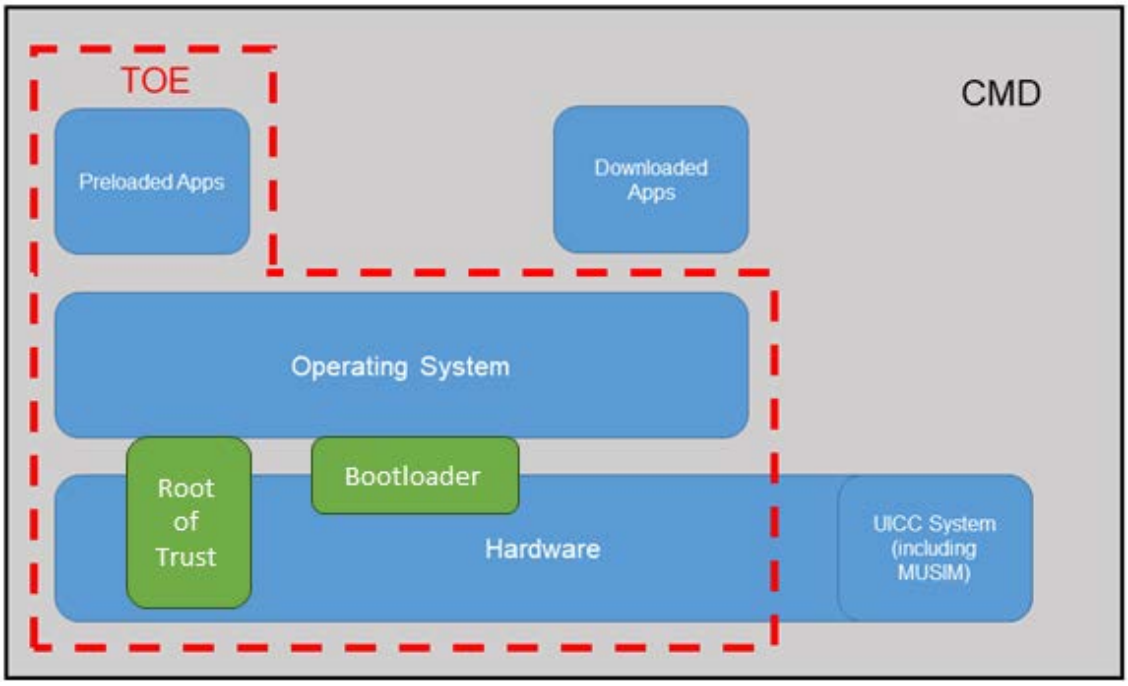


Figure 1: TOE boundary as defined in ETSI TS 103 732-1 [6]

The bootloader and Root of Trust are shown in green on the figure (the storage configuration are settings and not separate components easily defined in Figure 1).

These additional requirements provide a set of requirements focused on the operation of the bootloader and the Root of Trust, including how they protect the rest of the system. The assurance requirements paired with the functional requirements include ensuring how the CMD storage is configured for loading the next stage of the boot process (such as the kernel) and commands/arguments that may be passed to the boot sequence manually are documented and reviewed for security implications.

4.2 Usage and Major Security Features

This is a Protection Profile Module (PP-Module) used to extend a Base-PP for a consumer mobile device to provide additional security requirements on the bootloader.

The major security features are:

- Root of Trust: an intrinsically trusted component that is generated very early in the device start-up process (before the bootloader and other components are started) which can be used to provide integrity checks on later components to ensure the integrity of the system.
- Rollback protection: protection against the loading of a potentially vulnerable (but still TOE Manufacturer-approved at one point) version of the bootloader onto the system. A locked bootloader prevents this, or if authorized by the user, will ensure that user data is not available when the change is made.
- Boot modes and partitions: ensuring the integrity of the boot configuration on the device by specifically protecting the storage configuration and ensuring that the security functions of the device cannot be bypassed when booting into an alternate mode of operation (such as a recovery system).

4.3 PP-Module Identification

PP-Module Title	ETSI TS 103 732-5 (the present document) "Consumer Mobile Device; Part 5: Bootloader Protection Profile Module".
PP-Module Version	1.1.1
PP-Module Date	July 24, 2024

4.4 Base-PP Identification

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

Base-PP Short Name	[CMD PP]
Base-PP Title	ETSI TS 103 732-1 [6]: "Consumer Mobile Device; Part 1: Base Protection Profile".
Base-PP Version	2.1.2
Base-PP Date	November 16, 2023

4.5 Conformance Claim

The present document:

- claims conformance to CC V3.1 Release 5 [1], [2], [3], [4] and the CC and CEM addenda [5];
- is CC Part 2 [2] extended;
- assurance requirements are inherited from the Base-PP;
- does not claim conformance to any other PP.

5 Security Problem Definition

5.1 Assets and interfaces of the TOE

The TOE of this PP-Module is the bootloader and storage configuration on the CMD. The assets and interfaces of the TOE are defined in the Base-PP for the CMD, the TOE here is a deeper focus on the best security practices for the bootloader on the CMD to ensure those assets and interfaces are protected.

5.2 Threat agents and threats

The following threat agents from the Base-PP are identified as below:

- TA.PHYSICAL: a threat agent who has physical access to the TOE, and therefore to both the user interface and the physical interface.
- TA.FLAWAPP: a malicious or poorly programmed app that the user has installed on the TOE and that therefore has access to the application interface, and possibly to the local wireless interface and/or the wide-area network interface.

Threat Agents are limited to the Attack Potential of the Base-PP.

The following threats from the Base-PP are identified as below:

T.FLAWAPP_HACKS_TOE - TA.FLAWAPP attempts to modify the security behaviour of the TOE main OS.

T.PHYSICAL - TA.PHYSICAL attempts to gain access to *all* the assets by accessing physical interfaces of the TOE.

EXAMPLE: Physical interfaces include JTAG ports, USB (and similar) ports, charging ports, probing the PCB, direct access to the TOE storage media.

The following threats are added to those from the Base-PP:

T.INSECURE_INITIALIZATION - TA.PHYSICAL attempts to cause the execution of a malicious bootloader by manipulating the system in a way that compromises the Root of Trust.

T.RECOVER_DATA_ROLLBACK - TA.PHYSICAL attempts to install an older, vulnerable version of the TOE main OS that would allow compromise of the user data assets.

T. STORAGE_CORRUPTION - TA.PHYSICAL attempts to corrupt the storage utilized for by the TOE to bypass the security mechanisms of the boot process.

5.3 Organizational Security Policies

There are no organizational security policies defined for the TOE.

5.4 Assumptions

There are no assumptions defined for the TOE.

6 Security Objectives

6.1 Security Objectives for the TOE

The following security objectives from the Base-PP are identified as below as satisfied by the requirements in the PP-Module:

O.SECURE_BOOT - The TOE, at the start of its boot process, checks the TSF to ensure it has not been tampered with.

O.SECURE_WIPE - The TOE is able to make user data assets permanently unreadable.

O.SELF_PROTECTION - The TOE protects itself against apps attempting to modify TSF data and its security behaviour.

The following security objective is added to those from the Base-PP:

O.INITIALIZATION - The TOE shall be started through a secure initialization process that ensures the integrity and authenticity of the hardware settings and the initialization of the secure start-up of the Root of Trust functionality as well as the bootloader before it is executed.

O.ROLLBACK_PROTECTION - The TOE ensures that attempts to install older, vulnerable versions of the TOE main OS are prevented without user knowledge.

O. STORAGE_PROTECTION - The TOE protects the storage configuration against attempts to modify TSF data to bypass TSF enforcement.

6.2 Security Objectives for the Operational Environment

There are no security objectives for the operational environment.

6.3 Security Objectives Rationale

The security objectives rationales for threats that come from the Base-PP are in addition to the rationale in the Base-PP.

Threat	Rationale
T.FLAWAPP_HACKS_TOE (from the Base-PP)	This threat is countered by: • O.SELF_PROTECTION (from the Base-PP) by ensuring that the TSF security cannot be bypassed and that the bootloader does not have sufficient CPU privileges to provide an attack vector. • O.SECURE_BOOT (from the Base-PP) by ensuring that the Root of Trust integrity measurements are available for use during boot and that the storage configuration is protected against manipulation.
T.PHYSICAL (from the Base-PP)	This threat is countered by O.SECURE_BOOT (from the Base-PP) by ensuring that the Root of Trust integrity measurements are available for use during boot and that the storage configuration is protected against manipulation.
T.INSECURE_INITIALIZATION	This threat is countered by O.INITIALIZATION by requiring a secure initialization process to ensure the integrity and authenticity of the hardware configuration (including the Root of Trust) and bootloader before the bootloader can be executed.
T.RECOVER_DATA_ROLLBACK	This threat is countered by: • O.ROLLBACK_PROTECTION by ensuring that installing earlier versions of the main OS requires some form of user approval. • O.SECURE_WIPE by ensuring that changes to the bootloader configuration that would allow access requires the deletion of existing user data.
T. STORAGE_CORRUPTION	This threat is countered by O.STORAGE_PROTECTION by ensuring that the integrity of the storage configuration is protected.

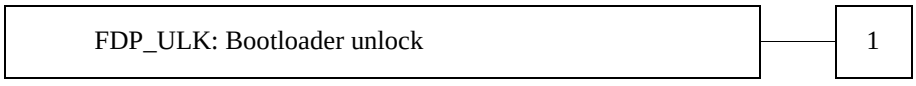
7 Extended Components Definition

7.1 Definition of the family Bootloader Unlock (FDP_ULK)

Family Behaviour

This family describes the functional requirements for how the user's data is protected when the bootloader is changed from a locked (when only developer-approved system images can be installed) to unlocked (when a non-developer-approved system image may be installed). The security functional components are defined in an additional family (FDP_ULK) of the Class FDP (User data protection).

Component Levelling



FDP_ULK.1 The TSF shall ensure that when changing the bootloader to an unlocked state that the user data is protected.

Management: FDP_ULK.1

There are no management activities foreseen.

Audit: FDP_ULK.1

There are no auditable events foreseen.

FDP_ULK.1 Bootloader unlock

Hierarchical to: No other components.

Dependencies: No dependencies.

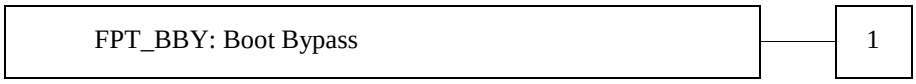
FDP_ULK.1.1 The TSF shall ensure that [selection: the bootloader cannot be unlocked, changing the bootloader to an unlocked state will wipe all user data].

7.2 Definition of the family Boot Bypass (FPT_BBY)

Family Behaviour

This family describes the functional requirements for how the bootloader shall not enable modes of operation which bypass the TSF. The security functional components are defined in an additional family (FPT_BBY) of the Class FPT (Protection of the TSF).

Component Levelling



FPT_ BBY.1 The bootloader shall not provide access to boot modes (such as a recovery mode) that would bypass the TOE Security Functions.

Management: FPT_BBY.1

There are no management activities foreseen.

Audit: FPT_BBY.1

There are no auditable events foreseen.

FPT_BBY.1 Boot Bypass

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_BBY.1.1 The TSF shall be enforced in any alternative boot modes.

7.3 Definition of the family Bootloader Privilege (FPT_BLP)

Family Behaviour

This family describes the functional requirements for how the bootloader is run within the CPU privilege levels. The security functional components are defined in an additional family (FPT_BLP) of the Class FPT (Protection of the TSF).

Component Levelling

FPT_BLP.1 The bootloader should run in the least privileged CPU privilege level possible.

Management: FPT_BLP.1

There are no management activities foreseen.

Audit: FPT_BLP.1

There are no auditable events foreseen.

FPT_BLP.1 Bootloader Privilege

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_BLP.1.1 The TOE bootloader shall be configured to run in the [assignment: *least privileged CPU privilege level*] of the processor.

7.4 Definition of the family TSF initialization (FPT_INI)

Family Behaviour

This family describes the functional requirements for the initialization of the TSF by a dedicated function of the TOE that ensures the initialization in a correct and secure operational state.

Component Levelling

This family consists of only one component, Component FPT_INI.1. This component requires the TOE to provide a TSF initialization function that brings the TSF into a secure operational state at power-on.

Management: FPT_INI.1

There are no management activities foreseen.

Audit: FPT_INI.1

There are no auditable events foreseen.

FPT_INI.1 TSF initialization

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_INI.1.1 The TOE shall provide an initialization function which is self-protected for integrity and authenticity.

FPT_INI.1.2 The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in FPT_INI.1.2 Table.

FPT_INI.1.2 Table

ID	Properties	Elements
1	[assignment: *property, for instance authenticity, integrity, correct version*]	[assignment: *list of TSF/user firmware, software or data*]

FPT_INI.1.3 The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE [selection: *is halted, successfully completes initialization with [*selection*: reduced functionality, signaling error state, [*assignment*: list of actions]*].

FPT_INI.1.4 The TOE initialization function shall only interact with the TSF in [assignment: *defined methods*] during initialization.

7.5 Definition of the family Partition Safety (FPT_PRT)

Family Behaviour

This family describes the functional requirements on the storage structure through the protection of and enforcement of the partition configuration of the TOE. The security functional components are defined in an additional family (FPT_PRT) of the Class FPT (Protection of the TSF).

Component Levelling

- FPT_PRT.1 The TSF shall protect the integrity of the partition configuration.
- FPT_ PRT.2 The TOE shall be configured to minimize the permissions assigned to partitions.

Management: FPT_PRT.1, FPT_PRT.2

There are no management activities foreseen.

Audit: FPT_PRT.1, FPT_PRT.2

There are no auditable events foreseen.

FPT_PRT.1 Partition protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PRT.1.1 The TSF shall protect the integrity of the partition configuration to prevent changes outside of the system image update process.

FPT_PRT.2 Partition restrictions

Hierarchical to: No other components.

Dependencies: FPT_PRT.1

FPT_PRT.2.1 The TOE has the following partitions marked as bootable: the main OS and [selection: *recovery, [*assignment: *other bootable partitions]*, *no other partitions*].

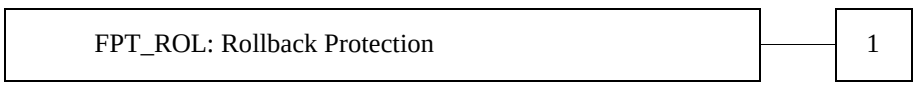
FPT_PRT.2.2 The TSF enforces restrictions on writing data, code execution and system permissions through the use of partition flags during the mounting of partitions for use by the TOE.

7.6 Definition of the family Rollback Protection (FPT_ROL)

Family Behaviour

This family describes the functional requirements for when and how the software/firmware on the device may allowed to have an older version of the software/firmware installed over a newer version (rollback). The security functional components are defined in an additional family (FPT_ROL) of the Class FPT (Protection of the TSF).

Component Levelling



FPT_ROL.1 The TSF shall only allow a software/firmware rollback under the specified conditions.

Management: FPT_ROL.1

There are no management activities foreseen.

Audit: FPT_ROL.1

There are no auditable events foreseen.

FPT_ROL.1 Rollback protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ROL.1.1 The TSF shall permit rollback of the system software and [selection: *tamper-evident storage firmware, [*assignment: *other software/firmware]*, *no other software/firmware*] under [selection: *all*, *no, [*assignment: *other conditions]*] conditions.

7.7 Definition of the family Root of Trust Data Integrity (FPT_RDI)

Family Behaviour

This family provides a requirement that address protection of Root of Trust data while it is stored within containers controlled by the TSF. Integrity errors may affect Root of Trust data stored in memory, or in a storage device.

Component Levelling

FPT_RDI: Root of Trust Data Integrity	1

FPT_RDI.1 Stored data integrity monitoring for the Root of Trust, requiring that the TSF monitor this data stored within containers controlled by the TSF for identified integrity errors.

Management: FPT_RDI.1

There are no management activities foreseen.

Audit: FPT_RDI.1

There are no auditable events foreseen.

FPT_RDI.1 Root of Trust Data Integrity

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RDI.1.1 The TSF shall monitor Root of Trust data stored in containers controlled by the TSF for integrity errors.

8 Security requirements

8.1 Conventions

The following conventions are used for the completion of operations defined in the SFRs:

- Unaltered SFRs are stated in the form used in Part 2 [2] or their Extended Component Definition (ECD).
- Refinement made in the PP: the refinement text is indicated with **bold text** and ~~strikethroughs~~.
- Selection wholly or partially completed in the PP: the selection values (i.e. the selection values adopted in the PP or the remaining selection values available for the ST) are indicated with UNDERLINED UPPERCASE TEXT:
  - e.g. '[selection: *disclosure, modification, loss of use*]' in Part 2 [2] or an ECD might become 'DISCLOSURE' (completion) or '[selection: DISCLOSURE, MODIFICATION]' (partial completion) in the PP.

- Assignment wholly or partially completed in the PP: *INDICATED WITH UPPERCASE ITALICIZED TEXT*.
- Assignment completed within a selection in the PP: the completed assignment text is indicated with *ITALICIZED AND UNDERLINED UPPERCASE TEXT*:
  - e.g. '[selection: change_default, query, modify, delete, [assignment: other operations]]' in Part 2 [2] or an ECD might become 'CHANGE_DEFAULT, *SELECT_TAG*' (completion of both selection and assignment) or '[selection: CHANGE_DEFAULT, *SELECT_TAG*, *SELECT_VALUE*]' (partial completion of selection, and completion of assignment) in the PP.
- Iteration: indicated by adding a string starting with '/' (e.g. 'FCS_COP.1/Hash').
- Extended SFRs are identified by having a label 'EXT' at the end of the SFR name.

8.2 ETSI TS 103 732-1 Security functional requirements

There are no modifications to the SFRs from the Base-PP.

8.3 TOE Security functional requirements

8.3.1 User data protection (FDP)

As the CMD is not a managed device in the enterprise sense, all management is handled locally by the user as opposed to a specific management service as would be the case for an enterprise device.

FDP_ULK.1 Bootloader Unlock

FDP_ULK.1.1 The TSF shall ensure that [selection: the bootloader cannot be unlocked, changing the bootloader to an unlocked state will wipe all user data].

Application Note 1: Unlocking the bootloader places the CMD into a state where the user may be able to install system images which are not signed by the developer. Not all CMDs support this capability.

8.3.2 Protection of the TSF (FPT)

FPT_ BBY.1 Boot Bypass

FPT_ BBY.1.1 The TSF shall be enforced in any alternative boot modes.

Application Note 2: Alternate boot modes are modes which do not boot to the main OS for normal functioning of the CMD. A common example of an alternate boot mode is a recovery mode which may provide a method for re-installing the system image (such as when an update has failed).

FPT_BLP.1 Bootloader Privilege

FPT_BLP.1.1 The TOE bootloader shall be configured to run in the [assignment: *least privileged CPU privilege level*] of the processor.

Application Note 3: The process to load the bootloader generally requires that it initially be loaded into the most privileged CPU privilege level (both due to it being one of the earliest programs to be loaded as well as to set the kernel with the appropriate privileges to execute). On many systems, once this is complete, a portion of the bootloader may remain in memory. The remaining bootloader program is placed into the CPU privilege level with the lowest privileges available, and is the level to be specified in the assignment.

FPT_INI.1 TSF initialization

FPT_INI.1.1 The TOE shall provide an initialization function which is self-protected for integrity and authenticity.

FPT_INI.1.2 The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in FPT_INI.1.2 Table.

FPT_INI.1.2 Table

ID	Properties	Elements
1	[*INTEGRITY*]	[*ROOT OF TRUST*]
2	[*PREVENTION OF DOWNGRADE TO PREVIOUS VERSIONS*]	[*ELEMENTS AS SPECIFIED IN FPT_ROL.1.1*]

FPT_INI.1.3 The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE [selection: *is halted, successfully completes initialization with [*selection*: reduced functionality, signaling error state, [*assignment*: list of actions]*].

FPT_INI.1.4 The TOE initialization function shall only interact with the TSF in [assignment: *defined methods*] during initialization.

FPT_PRT.1 Partition protection

FPT_PRT.1.1 The TSF shall protect the integrity of the partition configuration to prevent changes outside of the system image update process.

Application Note 4: The integrity of the partition configuration may be protected by functionality that is provided as part of FPT_TST.1 in the Base-PP.

FPT_PRT.2 Partition restrictions

FPT_PRT.2.1 The TOE has the following partitions marked as bootable: the main OS and [selection: *recovery, [*assignment: *other bootable partitions]*, *no other partitions*].

Application Note 5: Specific partition types are not required here. Main OS is the normal mode of operation. A recovery partition may not exist separately but may be included inside components of the main OS.

FPT_PRT.2.2 The TSF enforces restrictions on writing data, code execution and system permissions through the use of partition flags during the mounting of partitions for use by the TOE.

Application Note 6: Examples of partition options that should be described are read-only (ro), no execution (noexec) and no su (nosuid). All partitions should be documented to ensure the coverage of restrictions.

FPT_ROL.1 Rollback protection

FPT_ROL.1.1 The TSF shall permit rollback of the system software, and [selection: *tamper-evident storage firmware, [*assignment: *other software/firmware]*, *no other software/firmware*] under [selection: *all, no, [*assignment: *other conditions]*] conditions.

Application Note 7: The rollback prevention is not meant to prevent the rollback of application updates that are installed through the ADP but are related to the updates that are applied to change the main OS, bootloader and other components of the system. This is not meant to handle anything that is written into the partitions where applications and data are stored, only to the protected system software.

FPT_RDI.1 Root of Trust Data Integrity

FPT_RDI.1.1 The TSF shall monitor Root of Trust data stored in containers controlled by the TSF for integrity errors.

8.4 Security assurance requirements

There are no additional security assurance requirement beyond those defined in the Base-PP, though the following content expectations are clarified for ADV_FSP.2 Security-enforcing functional specification.

ADV_FSP.2 Security-enforcing functional specification clarification

As part of the functional specification, the interface between the bootloader and the kernel shall be considered as a TSFI. Boot arguments or commands that may be passed from the bootloader to the kernel outside those that are provided as part of the TOE configuration (such as arguments that may be passed by the user through an external connection to the device) shall be documented and reviewed.

8.5 Security requirements rationale

8.5.1 Rationale for choosing the SARs

This PP-Module does not define any additional assurance requirements above and beyond what is defined in the Base-PP that it extends. Application of the SARs to the TOE boundary described by both the claimed base and this PP-Module is sufficient to demonstrate that the claimed SFRs have been implemented correctly by the TOE.

8.5.2 The SFRs meet all the security objectives for the TOE

Security Objective	Rationale
O.SECURE_BOOT (from the Base-PP)	This objective is achieved by: • FPT_INI.1 and FPT_RDI.1, providing a Root of Trust to be used to verify the bootloader. • FPT_PRT.1 and FPT_PRT.2, protecting the integrity of the storage configuration.
O.SECURE_WIPE (from the Base-PP)	This objective is achieved by FDP_ULK.1, ensuring that user data cannot be accessed when the bootloader lock state is changed.
O.SELF_PROTECTION (from the Base-PP)	This objective is achieved by: • FPT_BBY.1, ensuring that all TSF capabilities are still enforced in alternate boot modes. • FPT_BLP.1, ensuring that the TOE bootloader does not have excess privileges such that it can be used to attack the system.
O.INITIALIZATION	This objective is achieved by FPT_INI.1 and FPT_RDI.1, providing a Root of Trust for the TOE prior to the execution of any other components.
O.ROLLBACK_PROTECTION	This objective is achieved by FPT_ROL.1, ensuring the bootloader cannot be downgraded or otherwise changed without direct user approval.
O.STORAGE_PROTECTION	This objective is achieved by: • FDP_ULK.1, by ensuring that changing the bootloader lock state cannot be changed without protecting the user data; • FPT_PRT.1 and FPT_PRT.2, protecting the integrity of the storage configuration.

8.5.3 Dependency analysis

SFR	Dependency	Rationale
FDP_ULK.1	-	
FPT_BBY.1	-	
FPT_BLP.1	-	
FPT_INI.1	-	
FPT_PRT.1	-	
FPT_PRT.2	FPT_PRT.1	Included in the PP-Module
FPT_RDI.1	-	
FPT_ROL.1	-	

8.6 Consistency rationale

8.6.1 TOE type consistency

When this PP-Module is used to extend the ETSI TS 103 732-1 [6] Base-PP, the TOE type for the overall TOE is still a consumer mobile device. This PP-Module adds requirements on bootloader and storage configuration included in the consumer mobile device. The TSF boundary is not extended, but provides more detailed requirements on components already included in the existing boundary.

8.6.2 Consistency of Security Problem Definition

The threats, OSPs and assumptions defined by the PP-Module are consistent with those defined in the ETSI TS 103 732-1 [6] Base-PP as follows.

PP-Module Threats/OSPs	Consistency Rationale
T.FLAWAPP_HACKS_TOE	These threats are taken from the Base-PP.
T.PHYSICAL	
T.RECOVER_DATA_ROLLBACK	The threat of data access based on downgrading the main OS components is a variation on the T.RECOVER_DATA threat, but focused on an active attack where the TA attempts to gain access to the user's data explicitly instead of accidentally.
T.STORAGE_CORRUPTION	The threat of Root of Trust data corruption is a variation of T.PHYSICAL.
T.INSECURE_INITIALIZATION	This threat of insecure initialization is related to T.PHYSICAL where the attack is focused on modifying TSF data such that the device is unable to ensure the integrity of the software/firmware being loaded.

8.6.3 Consistency of Objectives

The objectives for the preloaded applications are consistent with the ETSI TS 103 732-1 [6] Base-PP based on the following rationale.

PP-Module TOE Objectives	Consistency Rationale
O.SECURE_BOOT	These TOE Objectives are taken from the Base-PP.
O.SECURE_WIPE	
O.SELF_PROTECTION	
O.INITIALIZATION	This objective is a detailed subset of O.SECURE_BOOT focused specifically on the Root of Trust elements.
O.ROLLBACK_PROTECTION	This objective is a detailed subset of O.SECURE_BOOT focused specifically on local attempts to update the bootloader.
O. STORAGE_CONFIGURATION	This objective is a detailed subset of O.SELF_PROTECTION focused specifically on the Root of Trust elements.

8.6.4 Consistency of Requirements

The TOE of this PP-Module is comprised of the bootloader, storage configuration and Root of Trust elements described in clause 4.1. These comprise core functionality of the CMD.

This PP-Module assumes that the CMD satisfies SFRs defined in the ETSI TS 103 732-1 [6], and there are no specific SFR selections from ETSI TS 103 732-1 [6] that are required by the PP-Module. As the assurance and functional requirements in the PP-Module are additional to the ETSI TS 103 732-1 [6] requirements, there is no contradiction between the two sets of requirements.

History

Document history		
V1.1.1	July 2024	Publication