ETSI TS 103 732-4 V1.1.1 (2024-06)

CYBER;
Consumer Mobile Device;
Part 4: Preloaded Applications Protection Profile Module

Reference
DTS/CYBER-0083-4

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

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

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [6].

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.

Introduction

Consumer mobile devices like smartphones are becoming the entrance to digital services, such as mobile banking, electronic identity verification, digital key management, etc. Preloaded applications installed on the device provide many of these services for the user from the time the device is setup. As these applications are either included in the main OS or installed before the user completes the device set up, the manufacturer provides a measure of trustworthiness by documenting the preloaded applications and verifying the preloaded applications do not introduce security threats.

The present document identifies key focus areas around the applications preloaded on a consumer mobile device in typical consumer usage scenarios and identifies security threats to be mitigated in those applications. The identified threats are mitigated by security objectives, which are in their turn fulfilled by implementing appropriate security functional requirements.

The present document is defined as a Protection Profile Module (hereafter called PP-Module) following the structure from the CC standards [1], [2], [3] and therefore can be used for third party CC security assessments and certification. Notice that the present document has not been evaluated or certified as a formal PP-Module.

The requirements in the present document take published standards, recommendations and guidance in clause 2 into consideration.

1 Scope

The present document defines a PP-Module for Consumer Mobile Device (CMD) which adds additional security requirements on preloaded applications and the functional capabilities (objectives and security functional requirements) that are required to mitigate threats from poor programming of those applications.

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 set of preloaded applications 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".

[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:

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].

downloaded application: application installed by the choice of the user through an ADP

initial CMD setup: setup process that occurs when the device is either powered on by the consumer for the first time or after a factory reset and configures the device for first use, not including recovery or restore processes that may be invoked by the user

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].

preinstalled application: application provided by the TOE manufacturer installed without user intervention either prior to or during the initial CMD setup process

NOTE: Preinstalled applications are a type of downloaded applications and can be uninstalled by the user.

preloaded application: application provided by the TOE manufacturer as part of the system software that cannot be uninstalled by the user

production application: application ready for end user interaction instead of developer usage

security assurance requirements: description of how assurance is to be gained that the TOE meets the SFRs

NOTE: As defined in [1].

security functional requirement: 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].

system permission: permission granted by the main OS to manage itself (such as power off), provide core functions (such as SMS and Telephone), or access to underlying software and hardware interfaces

NOTE: As defined in [1].

system software: main OS, bootloaders, any preloaded apps and other components necessary for the device to function as expected

NOTE: As defined in [1].

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:

ADP	Application Distribution Platform
API	Application Program Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CMD	Consumer Mobile Device
ECD	Extended Component Definition
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

4 TOE Definition

4.1 TOE Overview

4.1.1 Introduction

This PP-Module introduces additional requirements on applications available on the CMD after the initial CMD setup is complete. The applications covered by these requirements are divided into preloaded and preinstalled applications. The requirements for preloaded applications are focused on defining security requirements to ensure they are trustworthy and maintained properly. The requirements for preinstalled applications are focused on how they are to be installed and maintained. Special focus is provided for preinstalled applications that are granted system permissions by the TOE manufacturer.

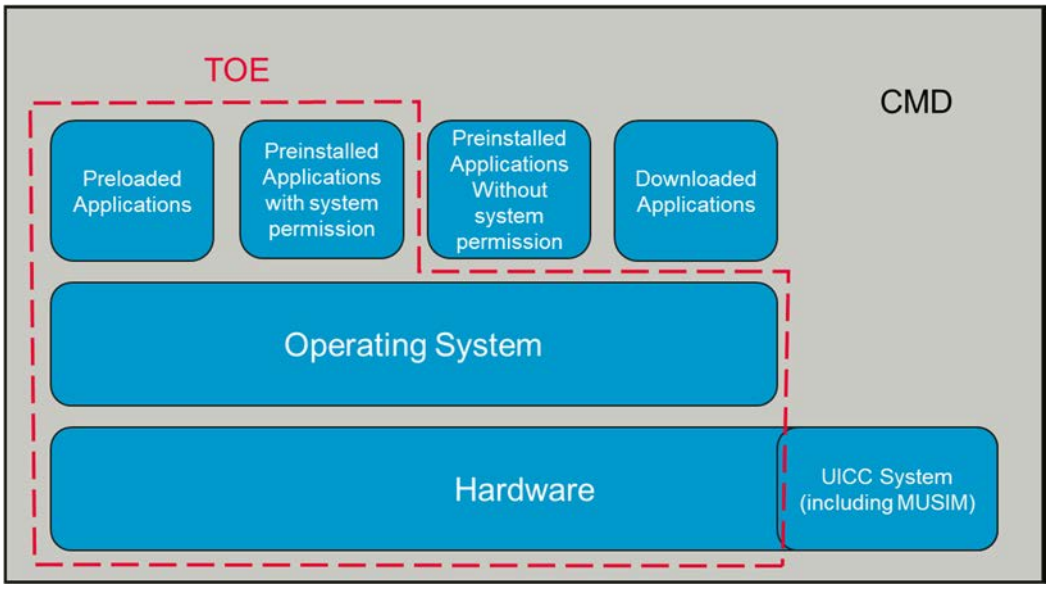


Figure 1: TOE boundary

Figure 1 illustrates the TOE boundary for the PP-Module (as it relates to the entire CMD). Preloaded applications as defined in ETSI TS 103 732-1 [6] are not changed. Preinstalled applications that are granted system permissions are included in the TOE.

4.1.2 Preloaded Application Requirements

This PP-Module introduces additional security requirements to the TOE as defined in ETSI TS 103 732-1 [6] specifically related to preloaded applications in the CMD. These additional requirements provide checks to the design of the preloaded applications to protect user and TSF data stored in the TOE.

4.1.3 Preinstalled Application Requirements

This PP-Module introduces additional security assurance requirements to the TOE as defined in ETSI TS 103 732-1 [6] specifically related to some preinstalled applications in the CMD.

The requirements for preinstalled applications are focused on the permissions assigned to such applications. Assigning system permissions on the CMD can act as an attack vector as a vulnerable application (whether intentionally or not) may provide additional access to the CMD than would be the case without the elevated permissions.

Additionally, during the initial CMD setup, the preinstalled applications that are downloaded should come from trustworthy Application Distribution Platforms (ADPs) as specified in ETSI TS 103 732-1 [6].

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 preloaded applications. As these applications are not explicitly chosen by the user, the manufacturer can provide additional assurance to the trustworthiness of the CMD by ensuring the applications meet these requirements.

The major security features are:

- Application Lifecycle: the update process for each preloaded application is defined to ensure it is maintained. When a preloaded application is uninstalled (which may leave an older version of the software available), the TOE provides information to the user about the implications of the removal. Preinstalled applications downloaded during the initial CMD setup need to be installed from a trustworthy location.
- Application Hardening: the preloaded applications follow best practices in development for the platform and are installed without unnecessary permissions to ensure that user or TOE data is protected.

- Preinstalled Application Permissions: preinstalled applications that are installed on the consumer mobile device and need to have additional system permissions shall be under the control of the TOE manufacturer.

4.3 PP-Module Identification

PP-Module Title	ETSI TS 103 732-4: "Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module".
PP-Module Version	1.1.1
PP-Module Date	June 11, 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: "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] and the CC and CEM addenda [5];
- is CC Part 2 [2] extended;
- assurance requirements are inherited from the Base-PP augmented with APA_LST.1;
- 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 set of preloaded applications and preinstalled applications with system permission on the CMD. The preinstalled applications with system permission are documented, but excluded from the scope of application testing. This PP-Module introduces new security requirements to the CMD to manage the preinstalled applications. 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 preloaded applications on the CMD to ensure those assets and interfaces are protected.

5.2 Threat agents and threats

The following threat agent in addition to those in the Base-PP is identified as below:

- TA.FLAWPREAPP: a poorly programmed application that is installed by the TOE manufacturer as part of the system software and 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 in addition to those in the Base-PP are identified as below:

T.APP_REVERSION - TA.LOCAL or TA.REMOTE attempts to access user data assets utilizing a TA.FLAWPREAPP that has been reverted to an earlier version with known flaws.

T.PERMISSIONS - TA.LOCAL or TA.REMOTE attempts to utilize system permissions assigned to a TA.FLAWPREAPP to gain elevated privileges on the TOE.

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

O.LIMITED_PERMISSIONS - The TOE shall provide system permissions only to the preinstalled applications under TOE manufacturer control.

O.OLD_APP_WARNING - The TOE shall provide the user with notifications when uninstalling updates from a preloaded application contained in the system software when an older version of the preloaded application is used.

6.2 Security Objectives for the Operational Environment

There are no security objectives for the operational environment.

6.3 Security Objectives Rationale

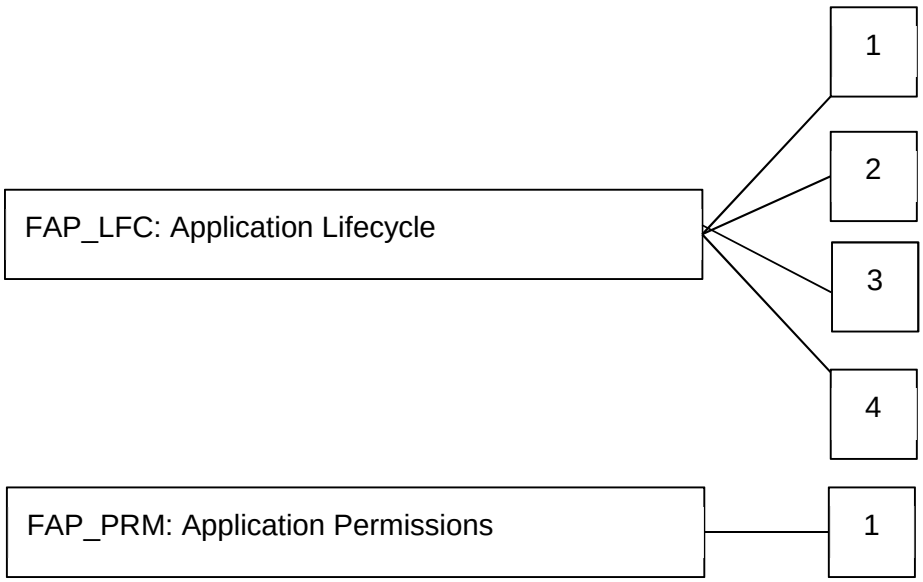
Threat	Rationale
T.APP_REVERSION	This threat is countered by O.OLD_APP_WARNING by ensuring the user is aware a preloaded application will be replaced by an older version if the preloaded application is part of the system software.
T.PERMISSIONS	This threat is countered by O.LIMITED_PERMISSIONS by ensuring that preinstalled applications are not granted system permissions available only to preloaded applications in in system software unless the preinstalled application is under the control of the TOE manufacturer.

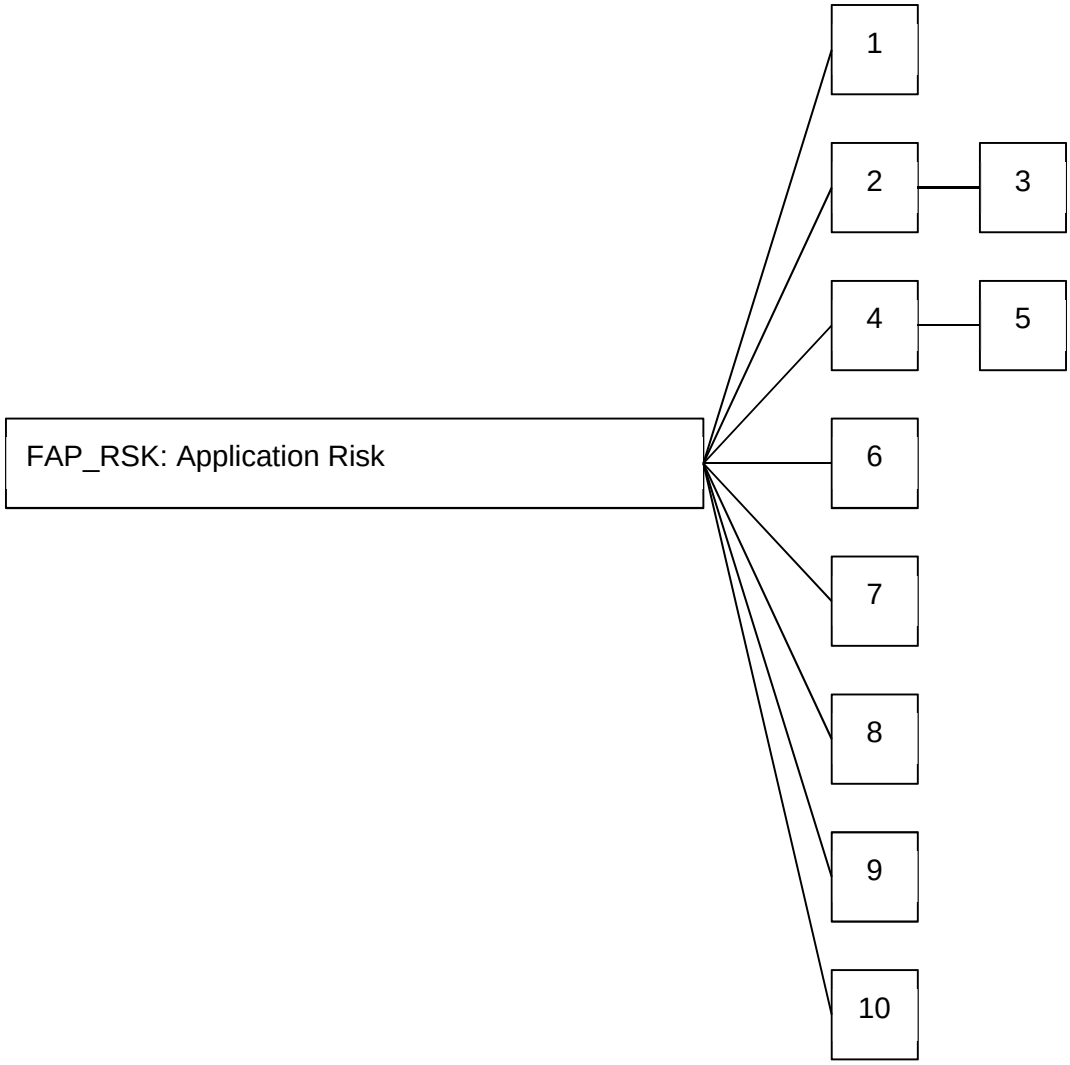
7 Extended Components

7.1 Definitions

7.1.1 Definition of the Class FAP: Applications

This class of requirements is focused on the risks associated with improperly designed applications. Applications are separate from the main operating system, though they may be included as part of the functionality provided on a consumer mobile device. Applications can provide unique attack vectors based on how they are designed and maintained on the device. The families relate to how applications are updated and configured.


FAP_LFC: Application Lifecycle
1
2
3
4
FAP_PRM: Application Permissions
1

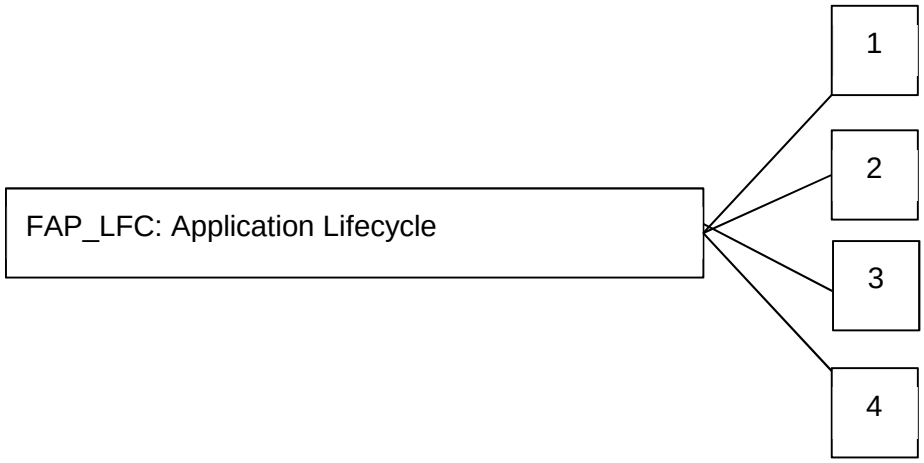

FAP_RSK: Application Risk
1
2
3
4
5
6
7
8
9
10

7.1.2 Definition of the family Application Lifecycle (FAP_LFC)

Family Behaviour

Applications need to be maintained to ensure flaws are corrected. This family defines requirements around how applications are updated and the actions that are taken when those updates are uninstalled (by the user).

Component Levelling



FAP_LFC.1 Preloaded applications are required to be updated to ensure flaws are remediated.

FAP_LFC.2 A preloaded application that is uninstalled will revert to the original version of the application contained in the system software. The user will be warned about using the original version and may have additional options or notices about using the application.

FAP_LFC.3 Preinstalled applications shall be updated from trusted ADPs.

FAP_LFC.4 Preinstalled applications downloaded as part of the initial CMD setup process shall be downloaded from trusted ADPs.

Management: FAP_LFC.1, FAP_LFC.2, FAP_LFC.3, FAP_LFC.4

There are no management activities foreseen.

Audit: FAP_LFC.1, FAP_LFC.2, FAP_LFC.3, FAP_LFC.4

There are no auditable events foreseen.

FAP_LFC.1 Preloaded application updates

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_LFC.1.1

The TSF shall ensure that preloaded applications are updated by [selection: *using an ADP and system software updates (to the version maintained in firmware), only by system software updates*].

FAP_LFC.2 Preloaded application uninstall

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_LFC.2.1

The TSF shall warn the user when a preloaded application update is uninstalled and the application will revert to the version in the system software, and allow the following actions: [selection: *disable the application (where possible), warn the user on the next use, none*].

FAP_LFC.3 Preinstalled application updates

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_LFC.3.1

The TSF shall ensure that preinstalled applications are only updated from the ADP(s) of the TOE manufacturer and/or OS developer.

FAP_LFC.4 Preinstalled applications download source

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_LFC.4.1

The TSF shall ensure that preinstalled applications are only downloaded from the ADP(s) of the TOE manufacturer and/or OS developer.

7.1.3 Definition of the family Application Permissions (FAP_PRM)

Family Behaviour

While all applications will have some set of permissions assigned (to access TOE services), some permissions are considered more dangerous than others in terms of protecting both the TOE and user data. This family defines how those permissions named system permission should be restricted.

Component Levelling

FAP_PRM.1

System permissions to TOE functionality are restricted only to all the preloaded applications and solely to the preinstalled application created by the TOE developer.

Management: FAP_PRM.1

There are no management activities foreseen.

Audit: FAP_PRM.1

There are no auditable events foreseen.

FAP_PRM.1 Restricted system permissions

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_PRM.1.1

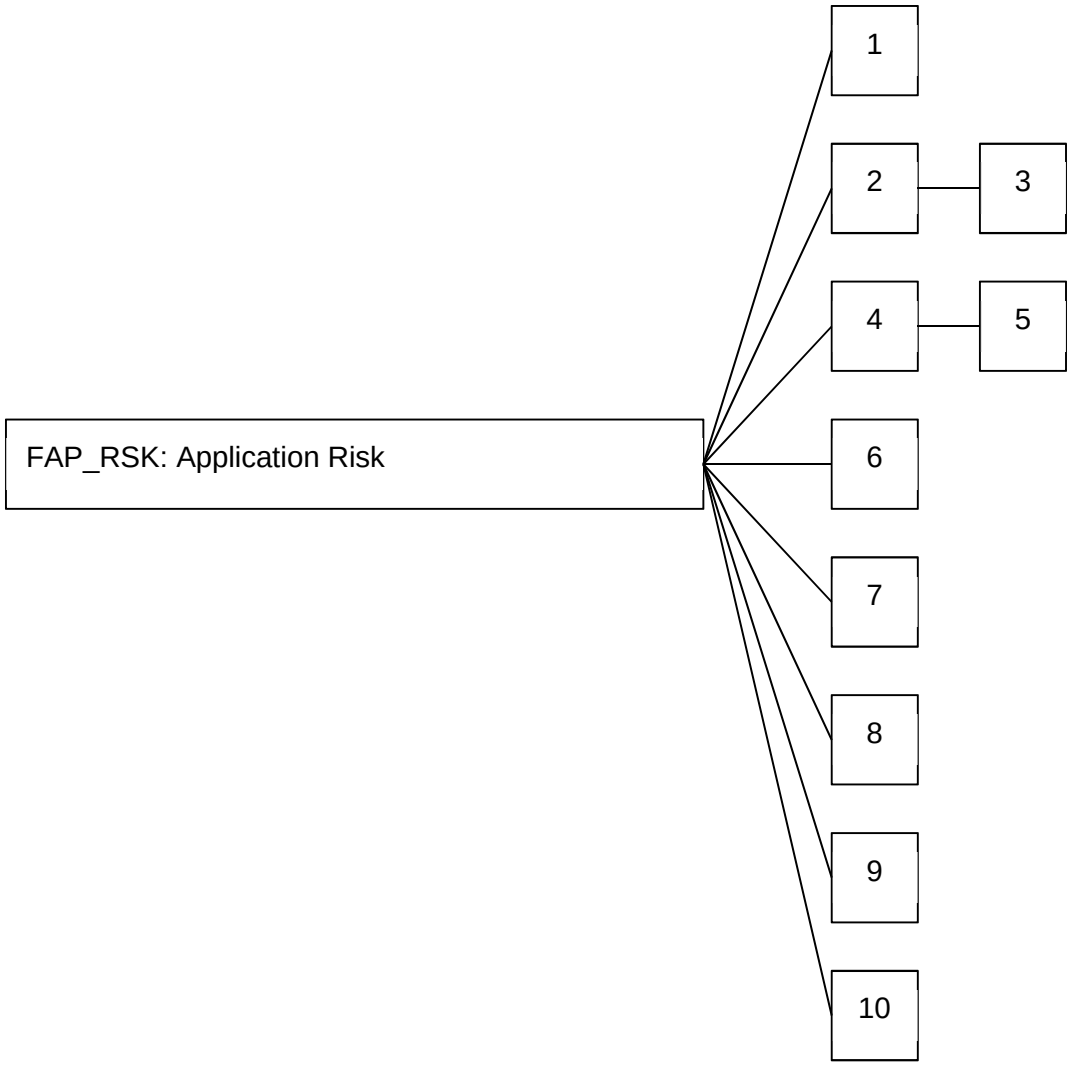
The TSF shall restrict the ability of applications to request [assignment: *permissions defined as system permission by the TOE developer*] to only preloaded applications and preinstalled applications created by the TOE developer.

7.1.4 Definition of the family Application Risk (FAP_RSK)

Family Behaviour

Applications are subject to specific risks related to common coding practices. Following best practices for application development ensures that core capabilities of the applications are correct.

Component Levelling



FAP_RSK.1 Applications are required to store data in prescribed locations and key storage systems.

FAP_RSK.2 Cryptographic functions require proper key generation algorithms.

FAP_RSK.3 Encryption of stored data is required to be done using properly generated cryptographic keys.

FAP_RSK.4 Network communications shall support the proper use of encryption for confidentiality as determined by the server endpoint.

FAP_RSK.5 Network communications require proper configurations to ensure protection of transmitted data.

FAP_RSK.6 To ensure a secure connection to the proper network endpoints, certificate checks shall be performed on the server certificate.

FAP_RSK.7 Application input, whether from APIs or the user, requires sanitization checks to prevent malformed data from being accepted.

FAP_RSK.8 Application data requires protection through all interfaces by which the data may be exposed from the device.

FAP_RSK.9 To establish applications are updated properly (from the correct source), valid signatures for the platform shall be provided with the installation package.

FAP_RSK.10 Debugging modes can expose application data, and so production applications are required to not be configured to be debuggable.

Management: FAP_RSK.1, FAP_RSK.2, FAP_RSK.3, FAP_RSK.4, FAP_RSK.5, FAP_RSK.6, FAP_RSK.7, FAP_RSK.8, FAP_RSK.9, FAP_RSK.10

There are no management activities foreseen.

Audit: FAP_RSK.1, FAP_RSK.2, FAP_RSK.3, FAP_RSK.4, FAP_RSK.5, FAP_RSK.6, FAP_RSK.7, FAP_RSK.8, FAP_RSK.9, FAP_RSK.10

There are no auditable events foreseen.

FAP_RSK.1 Application Data Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.1.1 The applications on the TOE shall only store data within their own storage context.

FAP_RSK.1.2 The applications on the TOE shall only store keys using the TSF-provided key storage.

FAP_RSK.2 Application Cryptographic Primitives

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.2.1 The applications on the TOE shall use appropriate cryptographic primitives to support the algorithms in use.

FAP_RSK.2.2 The applications on the TOE shall not use deprecated cryptographic modes or algorithms.

FAP_RSK.3 Application Hardcoded Keys

Hierarchical to: FAP_RSK.2

Dependencies: No dependencies.

FAP_RSK.3.1 The applications on the TOE shall not have hardcoded symmetric keys as the method of internal data protection.

FAP_RSK.4 Application Encrypted Connections

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.4.1 The applications on the TOE shall not have hardcoded unencrypted URLs for network communications.

FAP_RSK.5 Application Network Encryption

Hierarchical to: FAP_RSK.4

Dependencies: No dependencies.

FAP_RSK.5.1 The applications on the TOE shall use the trusted channels provided by FTP_ITC_EXT.1/HTTPS or FTP_ITC_EXT.1/TLS.

FAP_RSK.6 Application X.509 Certificate Validation

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.6.1 The applications on the TOE shall validate the X.509 server certificate according to the following rules:

- The certificate path shall terminate with a certificate in the TOE trust anchor.

- The TOE shall use the main OS-provided method to verify the certificate.

FAP_RSK.7 Application Sanitized Inputs

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.7.1 The applications on the TOE shall sanitize all input from external sources via any available interface.

FAP_RSK.8 Application Data Export

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.8.1 The applications on the TOE shall not support unauthorized direct access to data from external sources.

FAP_RSK.9 Application Signing

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.9.1 The applications on the TOE shall be signed with certificates in a signature format valid for the platform.

FAP_RSK.10 Application Debugging

Hierarchical to: No other components.

Dependencies: No dependencies.

FAP_RSK.10.1 The applications on the TOE shall not have any debug functionality enabled.

7.1.5 Definition of the Identification of applications on device (APA_LST)

Enumerating the preloaded and preinstalled applications with system permission is necessary to ensure how the operating system is separated from applications that are bundled as part of the system software. This family requires the developer to specify the applications from the TOE manufacturer that are available on the CMD at the completion of the initial CMD setup. This family should be included whenever evaluated CMDs include preloaded and/or preinstalled applications with system permission.

Application notes

This component requires the TOE developer to provide information on the applications which are available on the CMD at the completion of the initial CMD setup that are delivered by the TOE developer; this specifically excludes preinstalled applications without system permission.

The function of this component is to ensure the applications from the TOE developer available at the completion of the initial CMD setup are listed in terms of how they are classified (preloaded or preinstalled with system permission).

APA_LST.1 Application listing

Dependencies: No dependencies.

Developer action elements:

APA_LST.1.1D The developer shall provide a list of all preloaded and preinstalled applications with system permissions included on the consumer mobile device at the completion of the initial CMD setup.

Content and presentation elements:

APA_LST.1.1C The list of preloaded applications shall include all applications contained within the system software.

APA_LST.1.2C The list of preinstalled applications shall include all applications installed on the consumer mobile device at the completion of the initial CMD setup that have been assigned system permissions.

Evaluator action elements:

APA_LST.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation of sub-activity (APA_LST.1)

Objectives:

The objective of this sub-activity is to determine whether the set of preloaded and preinstalled applications with system permissions on the TOE after the initial CMD setup are listed.

Input:

The evaluation evidence for this sub-activity is:

a) the ST.

The list of all preloaded and/or preinstalled applications with system permissions may be provided as a table showing the information about each application. The applications may be provided as a list with the unique name of the application (not necessarily the application name presented to the user) and a version to uniquely identify the application as part of the TOE.

Action APA_LST.1.1E:

APA_LST.1.1C The list of preloaded applications shall include all applications contained within the system software.

APA_LST.1-1 The evaluator ***shall examine*** the ST to determine that it provides a list of all preloaded applications contained within the system software of the TOE. Components of the system software which are not applications are out of scope of this listing.

The evaluator ***shall compare*** the list of preloaded applications contained in the system software with those extracted by the evaluator.

APA_LST.1.2C The list of preinstalled applications shall include all applications installed on the consumer mobile device at the completion of the initial CMD setup that have been assigned system permissions.

APA_LST.1-2 The evaluator ***shall examine*** the ST to determine that it provides a list of all preinstalled applications that are installed during the initial CMD setup that have system permissions.

The evaluator ***shall compare*** the list of preinstalled applications with system permissions with those extracted by the evaluator after the completion of the initial CMD setup excluding the list of preloaded applications.

The evaluator ***shall verify*** that all preinstalled applications with system permissions on the consumer mobile device are included in the list of preinstalled applications.

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 Applications (FAP)

FAP_LFC.1 Preloaded application updates

FAP_LFC.1.1 The TSF shall ensure that preloaded applications are updated by [selection: *using an ADP and system software updates (to the version maintained in firmware), only by system software updates*].

FAP_LFC.2 Preloaded application uninstall

FAP_LFC.2.1 The TSF shall warn the user when a preloaded application update is uninstalled and the application will revert to the version in the system software, and allow the following actions: [selection: *disable the app (where possible), warn the user on the next use, none*].

Application note 1: The selection to warn the user on the next use is separate from the mandatory warning when the preloaded application updates are uninstalled. If the preloaded application does not support being uninstalled, then this is not applicable for that specific preloaded application. The requirement is not meant to be iterated for each preloaded application for when different options may be supported only on some actions.

FAP_LFC.3 Preinstalled applications updates

FAP_LFC.3.1 The TSF shall ensure that preinstalled applications are only updated from the ADP(s) of the TOE manufacturer and/or OS developer.

FAP_LFC.4 Preinstalled applications download source

FAP_LFC.4.1 The TSF shall ensure that preinstalled applications are only downloaded from the ADP(s) of the TOE manufacturer and/or OS developer.

Application note 2: While the ADP usually requires a user to login, the initial setup process may provide applications prior to any user account being created within the ADP.

FAP_PRM.1 Restricted system permissions

FAP_PRM.1.1 The TSF shall restrict the ability of applications to request [assignment: *permissions defined as system permission by the TOE developer*] to only preloaded applications and preinstalled applications created by the TOE developer.

8.3.2 Application Risk (FAP_RSK)

The Application Risk requirements defined here are targeted specifically at preloaded (not preinstalled) applications on the CMD. While the requirements are for generic applications, here they are specifically used for preloaded applications, and so all references to applications here are for preloaded applications.

FAP_RSK.1 Application Data Storage

FAP_RSK.1.1 The applications on the TOE shall only store data within their own storage context.

Application note 3: The storage context for an application may vary with the type of application. For applications that explicitly share output (for example the camera application), there may be two separate contexts; the application context for the configuration and settings of the application, and a shared context for the output from the application. The storage context for the application can be defined based on permissions or usage.

FAP_RSK.1.2 The applications on the TOE shall only store keys using the TSF-provided key storage.

Application note 4: While not included in the TOE boundary of the consumer mobile device, a UICC/eUICC is an acceptable TSF-provided key storage location.

FAP_RSK.2 Application Cryptographic Primitives

FAP_RSK.2.1 The applications on the TOE shall use appropriate cryptographic primitives to support the algorithms in use.

FAP_RSK.2.2 The applications on the TOE shall not use deprecated cryptographic modes or algorithms.

Application note 5: There is no single source defining algorithms as deprecated, but industry practice and standards bodies which define cryptographic algorithms periodically specify algorithms that no longer meeting current requirements. This requirement relies on those bodies' definition of deprecated algorithms.

FAP_RSK.3 Application Hardcoded Keys

FAP_RSK.3.1 The applications on the TOE shall not have hardcoded symmetric keys as the method of internal data protection.

FAP_RSK.4 Application Encrypted Connections

FAP_RSK.4.1 The applications on the TOE shall not have hardcoded unencrypted URLs for network communications.

Application note 6: While some services may be provided without encrypted communications, these should still not have hardcoded URLs that do not allow for updates in the future to encrypted communications.

FAP_RSK.5 Application Network Encryption

FAP_RSK.5.1 The applications on the TOE shall use the trusted channels provided by FTP_ITC_EXT.1/HTTPS or FTP_ITC_EXT.1/TLS.

Application note 7: This is not applicable for an application when the service being connected to does not provide encrypted channel support.

FAP_RSK.6 Application X.509 Certificate Validation

FAP_RSK.6.1 The applications on the TOE shall validate the X.509 server certificate according to the following rules:

- The certificate path shall terminate with a certificate in the TOE trust anchor;
- The TOE shall use the main OS-provided method to verify the certificate.

FAP_RSK.7 Application Sanitized Inputs

FAP_RSK.7.1 The applications on the TOE shall sanitize all input from external sources via any available interface.

FAP_RSK.8 Application Data Export

FAP_RSK.8.1 The applications on the TOE shall not support unauthorized direct access to data from external sources.

FAP_RSK.9 Application Signing

FAP_RSK.9.1 The applications on the TOE shall be signed with certificates in a signature format valid for the platform.

FAP_RSK.10 Application Debugging

FAP_RSK.10.1 The applications on the TOE shall not have any debug functionality enabled.

8.4 Security assurance requirements

In addition to the security assurance requirements defined in the Base-PP, the following assurance requirement is defined here (APA_LST.1).

APA_LST.1 Application listing

This component requires the TOE developer to provide information on the applications which are available on the CMD after the initial CMD setup is complete. The documentation provides categorization as to the origination of the application on the device (preloaded or preinstalled with system permission) for supporting the FAP_RSK security functional requirements.

Developer action elements:

APA_LST.1.1D The developer shall provide a list of all preloaded and preinstalled applications with system permissions included on the consumer mobile device at the completion of the initial CMD setup.

Content and presentation elements:

APA_LST.1.1C The list of preloaded applications shall include all applications contained within the system software.

APA_LST.1.2C The list of preinstalled applications shall include all applications installed on the consumer mobile device at the completion of the initial CMD setup that have been assigned system permissions.

Evaluator action elements:

APA_LST.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.5 Security requirements rationale

8.5.1 Rationale for choosing the SARs

This PP-Module defines an additional security assurance requirements family in addition to what is defined in the Base-PP. This class specifically adds activities around the preloaded and some preinstalled applications included in the TOE boundary for the TOE developer to complete. In combination with the SARs from the Base-PP, the additional SARs are 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.OLD_APP_WARNING	This objective is achieved by FAP_LFC.2 which specifies how users are warned when preloaded applications contained in the system software have their updates removed.
O.LIMITED_PERMISSIONS	This objective is achieved by FAP_PRM.1 by specifying system permissions and then excluding them from use by preinstalled applications not under the control of the TOE manufacturer.
O.ACCESS_CONTROL (from Base-PP)	This objective is achieved by: • FAP_RSK.1 specifies where application data is stored. • FAP_RSK.7 specifies that input is sanitized. • FAP_RSK.8 specifies that unauthorized direct access to application data is not allowed. • FAP_RSK.10 specifies that applications shall be published for production usage.
O.CRYPTOGRAPHY (from Base-PP)	This objective is achieved by FAP_RSK.2 to specify that proper cryptographic functions are used by the application.
O.PROTECT_COMMS (from Base-PP)	This objective is achieved by FAP_RSK.4, FAP_RSK.5 and FAP_RSK.6 which specify that network connections are protected and utilize well-defined protocols.
O.RANDOMS (from Base-PP)	This objective is achieved by FAP_RSK.3 by specifying the use of key generation.
O.SEPARATION (from Base-PP)	This objective is achieved by FAP_RSK.7 and FAP_RSK.10 by specifying that applications are protected from unauthorized input/access.
O.AUTHENTICATED_UPDATES (from Base-PP)	This objective is achieved by: • FAP_LFC.1 by specifying how the preloaded applications will be updated. • FAP_LFC.3 by specifying that preinstalled applications will be installed via a trusted ADP. • FAP_RSK.9 by specifying that applications be signed to ensure proper updating.

8.5.3 Dependency analysis

SFR	Dependency	Rationale
FAP_LFC.1	-	
FAP_LFC.2	-	
FAP_LFC.3	-	
FAP_PRM.1	-	
FAP_RSK.1	-	
FAP_RSK.2	-	
FAP_RSK.3	FAP_RSK.2	Included in the PP-Module
FAP_RSK.4	-	
FAP_RSK.5	FAP_RSK.4	Included in the PP-Module
FAP_RSK.6	-	
FAP_RSK.7	-	
FAP_RSK.8	-	
FAP_RSK.9	-	
FAP_RSK.10	-	

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 the preloaded and some preinstalled applications 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 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	Consistency Rationale
T.APP_REVERSION	The threat of downgrading system software applications is a subset of the T.NEW_ATTACKS threat in the Base-PP.
T.PERMISSIONS	This threat is related to T.FLAWAPP_ACCESS, T.FLAWAPP_HACKS_TOE and T.FLAWAPP_HACKS_OTHER_APPS in the Base-PP as it is one method through which these threats are possible.

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.LIMITED_PERMISSIONS	This TOE Objective is related to the O.SELF_PROTECTION objective in the Base-PP.
O.OLD_APP_WARNING	This TOE Objective is a specific subset of the O.AUTHETICATED_UPDATES objective in the Base-PP.

8.6.4 Consistency of Requirements

The TOE of this PP-Module is comprised of all the preloaded and TOE manufacturer preinstalled applications described in clause 4.1. The preloaded and TOE manufacturer preinstalled applications comprise both core functionality of the mobile device as well as additional functionality added by the TOE manufacturer.

This PP-Module assumes that the CMD satisfies SFRs defined in 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	June 2024	Publication