ETSI TS 103 732-3 V1.1.1 (2023-10)

CYBER;
Consumer Mobile Device;
Part 3: Multi-user Protection Profile Module

Reference
DTS/CYBER-0083-3

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 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [4].

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. Meanwhile more and more security attack vectors are being explored, such as malicious applications, network eavesdropping. Defining security and assurance requirements for mobile devices can mitigate potential risks and drive the mobile device security to an appropriate level in order to protect users of such mobile devices.

The present document identifies key assets to be protected in typical consumer usage scenarios and identifies security threats associated to these key assets. 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 (hereafter called PP) following PP 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.

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) Multi-user, which adds support for multiple unique users to the CMD each with separate authentication and (shared, but isolated) storage.

The PP-Module identifies the key aspects needed to support multi-user capabilities on the CMD platform and identifies the threads associated to them and the functional capabilities (objectives and security functional requirements) that are required to mitigate those threats.

The Target Of Evaluation (TOE) described by the present document is a consumer mobile device as enhanced by support for multiple users.

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] ETSI TS 103 732-1 (V2.1.1): "CYBER; Consumer Mobile Device; Part 1: Base Protection Profile".

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

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

lock screen: screen that is displayed when the device is locked and requires credentials to be entered to access the primary functionality of the TOE

lock screen(boot): screen that is displayed when the device is locked after the device has been (re)started, prior to any user successfully entering any credentials

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

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

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].

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

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
ECD	Extended Component Definition
EMM	Enterprise Mobility Management
FDP	Functional class user Data Protection
FIA	Functional class Identification and Authentication
FMT	Functional class security Management
GSM	Global System for Mobile
MUSIM	Multi-(U)SIM
OS	Operating System

PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality

4 TOE Definition

4.1 TOE Overview

The TOE type remains as described in [CMD PP].

The usage and major security features of the TOE generally remains as described in [CMD PP].

This PP-Module introduces the scenario where the main OS supports multiple users. Different users are likely to have different privileges. Most likely, the level of privileges will be determined by the order of the user account creation, though this is not required.

While it is not necessary to have users with different privileges on the device, the unmanaged nature of the consumer device (e.g. no EMM is used to control the configuration), it is likely the one account will have some level of additional privileges (a simplified management system). For simplicity, the following role definitions will be used to provide common terms for differently privileged accounts:

- **owner role:** account that is normally the same as a primary role, but is explicitly associated with the first account created on the device during the initial device setup
- **primary role:** account that has the privileges necessary to "manage" the device (the primary role account would usually be considered the "**owner**" of the device though this is not mandatory)
- **secondary role:** account that has privileges to login on the device, but cannot perform "management" functions
- **guest role:** account which does not require login credentials, does not have any "management" privileges and which all saved data is deleted when the account is logged out (such as when restarting the device, or maybe when switching active user accounts)

There is no restriction on the number of accounts that can be defined at any role (though usually there is only a single guest account since no stored profile is maintained). Additional roles can be provided, and privileges assigned as appropriate for the expected usage.

The TOE developer shall define the TOE clearly as part of submission for CC evaluation.

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 that implements Multi-User functionality. Therefore, the Target of Evaluation (TOE) in this PP-Module is a mobile device that implements Multi-User functionality.

Management privileges are normally going to be limited, and would normally fall into one of these categories:

- Creation of additional primary or secondary accounts.
- Enabling Guest account functionality.
- Controlling sharing of data between accounts (for example a shared photo album).

- Device-wide configurations (such as Wi-Fi available to the whole device, or Bluetooth devices available to any user).

Other functions may be available, or these functions may be split among different roles (for example device-wide configurations may be something that any user can add to, while only primary users can delete).

The major security features of this PP-Module are:

- Multiple user support: the TOE can support (this is specifically multiuser support inside the main OS and not related to MUSIM or embedded components that may support multiple users):
  - multiple roles (such as providing a primary user that can manage other user accounts); and
  - independent user accounts on the device such that the data for each account is protected from access by other accounts.

4.3 PP-Module Identification

PP-Module Title	ETSI TS 103 732-3: "Consumer Mobile Device; Part 3: Multi-user Protection Profile Module"
PP-Module Version	1.1.1
PP-Module Date	October 23, 2023

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 [4]: "Consumer Mobile Device; Part 1: Base Protection Profile"
Base-PP Version	2.1.1
Base-PP Date	October 23, 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 and CC Part 3 [3] extended;
- inherits all assurance requirements from the Base-PP;
- does not claim conformance to any other PP.

5 Security Problem Definition

5.1 Assets and interfaces of the TOE

In addition to the assets to be protected as defined in the Base-PP, the following assets are protected in the PP-Module:

- Individual user data assets stored in the TOE:
  - user data: files, photos, videos, notifications, etc.

Interfaces of the TOE are defined in the Base-PP.

5.2 Threat agents and threats

The Threat Agents for this PP-Module are (a more limited set from the Base-PP):

- TA.PHYSICAL: a threat agent who has physical access to the TOE, and therefore to both the user interface and the physical interface.

The threats for this PP-Module are identified as below:

T.ACCESS_USERDATA - A threat agent might gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy.

T.ACCESS_TSFFUNC - A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.

5.3 Organizational Security Policies

This PP-Module does not add any organizational security policies to what is in the Base-PP.

5.4 Assumptions

This PP-Module does not add any assumptions to what is in the Base-PP.

6 Security Objectives

6.1 Security Objectives for the TOE

O.DATA_SEPARATION - The TOE will ensure that user data is only accessible to the owner of the data.

O.DISCRETIONARY_ACCESS - The TOE will control access of subjects and/or users to named resources based on identity of the object. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.

6.2 Security Objectives for the Operational Environment

This PP-Module does not add any security objectives for the operational environment to what is in the Base-PP.

6.3 Security Objectives Rationale

Threat	Rationale
T.ACCESS_USERDATA	This threat is countered by O.DATA_SEPARATION ensuring that only authenticated user can access the device functionality.
T.ACCESS_TSFFUNC	This threat is countered by O.DISCRETIONARY_ACCESS ensuring that only authenticated user can access the device functionality.

7 Extended Components Definition

None defined.

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 [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 text
  - e.g. "[selection: *disclosure, modification, loss of use*]" in [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 italicized text
- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text*
  - e.g. "[selection: change_default, query, modify, delete, [assignment: other operations]]" in [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. "FDP_ACC.2/Multi")
- Extended SFRs are identified by having a label "EXT" at the end of the SFR name.

8.2 Base-PP Security Functional Requirement Direction

8.2.1 Introduction

In a PP-Configuration that includes the ETSI TS 103 732-1 [4], the multi-user functionality is expected to rely on some of the security functions implemented in the CMD as a whole and evaluated against the Base-PP. While the PP-Module does not require any changes to the requirements of the Base-PP, it does rely on several key components to fully implement the requirements specified here.

8.2.2 Authentication

The PP-Module does not implement any requirements targeting authentication functionality. In an evaluated CMD using a PP-Configuration including this PP-Module, the authentication system is expected to support multiple users on the device instead of a single user.

The authentication functionality provided for each additional user on the TOE should be the same, but if it is not, any differences should be documented for the evaluation.

8.2.3 Permissions Policy

The access control policy from the PP-Module should work together with the Permissions Policy from the Base-PP to integrate separate user accounts as a variable in the access control list associated with the permissions policy.

8.2.4 Management User Controls

The management functions listed as user controls should be able to be set for each user. For example, notification settings should be unique to each user on the device.

8.3 Security functional requirements

8.3.1 Multi-User requirements

8.3.1.1 User Data Protection (FDP)

FDP_ACC.2/Multi Complete access control

FDP_ACC.2.1/Multi The TSF shall enforce the [*Discretionary Access Control Policy*] on [

- *subjects: processes acting on behalf of a user;*
- *objects: Apps and files*].

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/Multi The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/Multi Security attribute based access control

FDP_ACF.1.1/Multi The TSF shall enforce the [*Discretionary Access Control Policy*] to objects based on the following: [*The user identity and privilege(s) associated with a subject*].

FDP_ACF.1.2/Multi The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *the subject is the owner of the object;*
- *the subject has been granted access to the object by the object owner or a primary role account*].

FDP_ACF.1.3/Multi The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*if the subject has privileges to provide access to the object*].

FDP_ACF.1.4/Multi The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*the subject is not explicitly granted access to the object*].

8.3.1.2 Security Management (FMT)

FMT_MSA.1/Multi Management of security attributes

FMT_MSA.1.1/Multi The TSF shall enforce the [*Discretionary Access Control Policy*] to restrict the ability to [create, modify, delete] the security attributes **[selection: *secondary role user accounts, guest role user accounts and [assignment: ~~list of security attributes~~ other role user accounts]*]** to [*primary role user accounts*].

FMT_MSA.3/Multi Static attribute initialization

FMT_MSA.3.1/Multi The TSF shall enforce the [*Discretionary Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Multi The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Application Note 1: "restrictive" is specified as by default accounts should not share any data unless explicitly authorized.

FMT_SMF.1/Multi Specification of Management Functions

FMT_SMF.1.1/Multi The TSF shall be capable of performing the following management functions: [

- *create new user accounts;*
- *enable/disable user accounts;*

- *delete user accounts;*
- *enable/disable guest accounts;*
- *assign permission of applications for non-primary role user accounts;*
- *[assignment: other management functions]*].

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [~~assignments~~**selection:** *owner, primary, secondary, guest and [assignment: other roles]*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

8.4 Security requirements rationale

8.4.1 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.

8.4.2 The SFRs meet all the security objectives for the TOE

Security Objective	Rationale
O.DATA_SEPARATION	This objective is achieved by: • FDP_ACC.2/Multi specifies the policy to access data. • FDP_ACF.1/Multi specifies the policy to access data. • FMT_MSA.1/Multi specifying that only the primary role user account can create, modify, delete other user accounts. • FMT_SMR.1 specifying that the user can define roles and accounts on the device.
O.DISCRETIONARY_ACCESS	This objective is achieved by: • FDP_ACC.2/Multi • FDP_ACF.1/Multi • FMT_MSA.3/Multi • FMT_SMF.1/Multi All of which describes the discretionary access control policy specifying authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.

8.4.3 Dependency analysis

SFR	Dependency	Rationale
FDP_ACC.2/Multi	FDP_ACF.1/Multi	
FDP_ACF.1/Multi	FDP_ACC.2/Multi FMT_MSA.3/Multi	
FMT_MSA.1/Multi	FDP_ACC.2/Multi FMT_SMR.1 FMT_SMF.1/Multi	FMT_SMR.1
FMT_MSA.3/Multi	FMT_MSA.1/Multi FMT_SMR.1	
FMT_SMF.1/Multi	-	
FMT_SMR.1	FIA_UID.1	Fulfilled by FIA_UID.1 in the Base-PP

Annex A (informative): Bibliography

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

History

Document history		
V1.1.1	October 2023	Publication