ETSI TS 103 932-1 V1.1.2 (2023-11)

TECHNICAL SPECIFICATION

**CYBER;
Consumer Mobile Devices Base PP-Configuration;
Part 1: CMD and Biometric Verification**

Reference

RTS/CYBER-00125

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

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or
other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

ETSI

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 1 of a multi-part deliverable covering Consumer Mobile Devices Base PP-Configuration.

NOTE: At the time of the publication of the present document, the other parts are under development.

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.

Executive summary

The present document specifies the evaluation configuration for a CMD when using a biometric system for authentication. The Protection Profile Configuration (PP-Configuration) documents the requirements for merging the requirements of the two documents so a product can be evaluated as a whole.

Introduction

The purpose of a PP-Configuration is to define a Target Of Evaluation (TOE) that combines Protection Profiles (PPs) and Protection Profile Modules (PP-Modules) into a single configuration that can be evaluated as a whole. The scope includes the definition of the configuration of a Consumer Mobile Device (CMD) that has biometric verification and enrolment functionality.

# 1		Scope

The present document is the PP-Configuration for the combination of the Consumer Mobile Device PP and the Biometric Authentication PP-Module.

# 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".

[7]		ETSI TS 103 732-2 (V1.1.2): "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".

## 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

Void.

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
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation

4   PP-Configuration Reference

This PP-Configuration is identified as follows:

PP-Configuration Short Name	CFG_CMD_BIO
PP-Configuration Title	ETSI TS 103 932-1: "Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification".
PP-Configuration Version	1.1.2
PP-Configuration Date	November 16, 2023

5   PP-Configuration Components Statement

This PP-Configuration includes the following components:

- Base-PP: ETSI TS 103 732-1 [6]: "Consumer Mobile Device; Part 1: Base Protection Profile", November 16, 2023, V2.1.2

- PP-Module: ETSI TS 103 732-2 [7]: "Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module", November 16, 2023, V1.1.2

6   Conformance Claim and Statement

6.1   Common Criteria Conformance Claim

This PP-Configuration, the Base-PP and the PP-Module are conformant to Common Criteria Version 3.1, Revision 5 [1], [2], [3], and [4] as extended by the requirements in each document.

6.2   Conformance Type

To be conformant to this PP-Configuration, the Security Target shall demonstrate Exact Conformance as defined by "CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs", Version 0.5, May 2017 CCDB-2017-05-xxx [5].

6.3   Assurance Package Conformance Claim

In order to evaluate a TOE that claims conformance to this PP-Configuration, the evaluator shall evaluate the TOE against the following SARs that are defined in the Base-PP.

Assurance Class	Assurance Components
Development (ADV)	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design
Guidance documents (AGD)	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Life-cycle Support (ALC)	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures ALC_DVS_EXT.1 Identification of security measures (extended) ALC_FLR.3 Systematic flaw remediation (refined)
Security Target evaluation (ASE)	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition
Tests (ATE)	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	AVA_VAN.2 Vulnerability analysis

History

Document history		
V1.1.1	October 2023	Publication
V1.1.2	November 2023	Publication