ETSI TS 103 732-2 V1.1.2 (2023-11)

CYBER;
Consumer Mobile Device;
Part 2: Biometric Authentication Protection Profile Module

Reference
RTS/CYBER-00124

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 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [5].

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 generally provide biometric systems for easy authentication of the user(s) of the device. Biometric systems can use a wide range of characteristics of the user, from fingerprints to face, each with its own unique set of capabilities. A key measure of the quality of any biometric system and its ability to protect assets is the accuracy of its matching capabilities. The false accept and reject rates provide measures about the trustworthiness of the system when implemented on a device to provide protection against threats to casual impersonation attacks.

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 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.

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 the capability to use biometric characteristics for authentication.

The present document identifies key assets of the biometric system of the CMD to be protected and identifies the threats associated to them and the functional capabilities (objectives and security functional requirements) that are required to mitigate those threats.

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 a biometric system incorporated into a CMD. Presentation Attack Detection is excluded from the scope of this TOE.

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

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

[6] Biometrics Security iTC: "Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOSD]", version 1.1, September 12, 2022.

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:

authentication factor: general term that can stand for any input used to verify a user as an authentication credential. There are three types of possible factors:

- **biometric authentication factor:** use of a biometric sample matched to template generated by an enrolment process (and possibly updated during successful authentication attempts);
- **external authentication factor:** use of a separate item in possession of the user to provide authentication such as a security key;
- **known authentication factor:** use of something the user knows, a password, PIN or pattern for authentication.

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].

separate execution environment: operating environment separate from the main OS with highly restricted access used to provide secure isolation for sensitive operations

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:

BAF	Biometric Authentication Factor
CC	Common Criteria
CEM	Common Evaluation Methodology
CMD	Consumer Mobile Device
EAF	External Authentication Factor
ECD	Extended Component Definition
FAR	False Acceptance Rate
FIA	Functional class Identification and Authentication
FMR	False Match Rate
FMT	Functional class Security Management
FNMR	False Non-Match Rate
FRR	False Rejection Rate
KAF	Known Authentication Factor
OS	Operating System
PIN	Personal Identification Number
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

This PP-Module introduces additional major security features of the TOE for user authentication using biometric information, which protect user and TSF data stored in the TOE. This includes both biometric enrolment and verification of the user. The TOE is a component of a larger TOE environment that is defined by the TOE of the Base-PP (a CMD) in ETSI TS 103 732-1 [5].

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 biometric enrolment and verification to unlock a locked mobile device using the user's biometric characteristics.

To enable biometric authentication, the TOE shall first enrol a user's biometric characteristics to create a template used for verification. The process of enrolment collects samples from the user (such as images or scans based on the biometric modality sensor) and uses this input to generate the template used as the biometric authentication credential for the user. Enrolment requires the user to already be authenticated with a Known or External Authentication Factor (KAF or EAF). The TOE does not place any limits as to the number of templates that may be created or whether or how they may be labelled.

A user presents their biometric characteristic to the TOE for verification without any additional identifying information (such as a username). The TOE captures the sample from the user and extracts biometric characteristics and compares them to all the stored templates to determine whether the presented sample results in a successful match (or a failure to match). The result of the verification is returned to the calling component of the CMD.

The major security features are:

- Biometric enrolment: the TOE provides the capability to enrol a biometric characteristic to generate a template to be used as the authentication credentials:
  - Credential management: the TOE provides the ability for the user to manage their enrolled template(s).
- Biometric verification: the TOE provides the capability to verify if a presented sample for user authentication matches a stored template.

4.3 PP-Module Identification

PP-Module Title	ETSI TS 103 732-2: "Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".
PP-Module Version	1.1.2
PP-Module Date	November 16, 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 [5]: "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 [4];
- is CC Part 2 [2] extended;
- inherits all assurance requirements from the Base-PP;
- does not claim conformance to any other PP.

4.6 Evaluation Activities

The extended requirements in this PP-Module use the evaluation activities defined in the "Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOSD]" [6].

5 Security Problem Definition

5.1 Assets and interfaces of the TOE

The TOE of this PP-Module is the biometric subsystem included in the CMD. As such, the assets and interfaces of the TOE are defined in the Base-PP for the CMD, and the TOE here is another authentication option available for the user of the device.

5.2 Threat agents and threats

Threat Agents:

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

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

The threats are identified as below:

- **T.BIO_IMPERSONATE -** TA.PHYSICAL impersonates the legitimate user without being enrolled in the TOE to gain access to user data assets.

5.3 Organizational Security Policies

P.ENROL - The TOE shall enrol a user for biometric verification only after successful authentication of the user with a KAF or EAF.

P.VERIFICATION - The TOE shall meet relevant criteria for its security relevant error rates for biometric authentication.

5.4 Assumptions

There are no assumptions defined for the TOE.

6 Security Objectives

6.1 Security Objectives for the TOE

O.BIO_VERIFICATION - The TOE will verify the user identity using a mechanism that meets the relevant criteria for security relevant error rates for the verification process.

O.ENROL - The TOE shall implement the functionality to enrol a user for biometric verification only after successful authentication of the user with a KAF or EAF.

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.BIO_IMPERSONATE **P.VERIFICATION**	This threat and policy are countered by O.BIO_VERIFICATION ensuring that only properly enrolled users can authenticate to the device.
P.ENROL	This policy is enforced by O.ENROL to require the user shall be properly authenticated prior to enrolment.

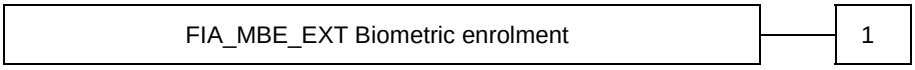
7 Extended Components Definition

7.1 Definition of the family Biometric enrolment (FIA_MBE_EXT)

Family behaviour

This component defines the requirements for the TSF to be able to enrol a user, create templates of sufficient quality and prevent presentation attacks.

Component levelling



FIA_MBE_EXT.1, Biometric enrolment requires the TSF to enrol a user.

Management: FIA_MBE_EXT.1

There are no management activities foreseen.

Audit: FIA_MBE_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the base PP/ST:

a) Basic: Success or failure of the biometric enrolment.

FIA_MBE_EXT.1 Biometric enrolment

Hierarchical to: No other components.

Dependencies: No dependencies.

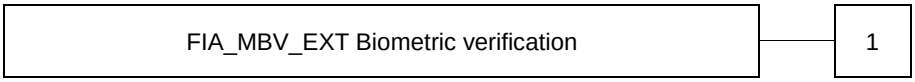
FIA_MBE_EXT.1.1 The TSF shall provide a mechanism to enrol an authenticated user to the biometric system.

7.2 Definition of the family Biometric verification (FIA_MBV_EXT)

Family behaviour

This clause describes the functional requirements for the TSF to be able to verify a user, use samples of sufficient quality and prevent presentation attacks.

Component levelling



FIA_MBV_EXT.1, Biometric verification requires the TSF to verify a user.

Management: FIA_MBV_EXT.1

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

a) the management of the TSF data (setting threshold values) by an administrator.

Audit: FIA_MBV_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the base PP/ST:

a) basic: Success or failure of the biometric verification.

FIA_MBV_EXT.1 Biometric verification

Hierarchical to: No other components.

Dependencies: FIA_MBE_EXT.1 Biometric enrolment.

FIA_MBV_EXT.1.1 The TSF shall provide a biometric verification mechanism using [selection: *fingerprint, eye, face, voice, vein,* [assignment: *other biometric modality*]].

FIA_MBV_EXT.1.2 The TSF shall provide a biometric verification mechanism with the [selection: *FMR, FAR*] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*].

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 CC 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 CC 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 CC 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

8.2.1 Modified SFRs

In a PP-Configuration that includes the ETSI TS 103 732-1 [5] PP, the biometric enrolment and verification is expected to be added to the authentication mechanisms supported by the mobile device. In this case, the following clauses describe any modifications that the ST author shall bake to the SFRs defined in the Base-PP in addition to what is mandated in clause 8.3.

The refinements in the SFRs (to the base-PP) are in **bold** text.

8.2.2 Identification and Authentication (FIA)

FIA_UAU.5/Local Multiple authentication mechanisms

FIA_UAU.5.1/Local The TSF shall provide [*PASSWORD, PIN* and selection: *PATTERN, **2D FACE, 3D FACE, FINGERPRINT**, [assignment: EAF], NO OTHER MECHANISM*] to support user authentication.

Application Note 1: Use of an EAF assumes that the EAF is trusted by the user and so its security is out of scope of the evaluation. The use of the EAF shall be described and the connection to the TOE shall be stated (for example, over a wired connection or the particular wireless protocol used).

FIA_UAU.5.2/Local The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

Application Note 2: Rules can be: "Always try **biometric** authentication first", "Always require both password and **biometric** authentication", "User chooses which mechanism to use", etc.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [*AN INTEGER BETWEEN 3 AND 10*] unsuccessful authentication attempts occur related to [~~assignment: list of authentication events~~ selection: *PASSWORD, PIN, PATTERN, **2D FACE, 3D FACE, FINGERPRINT**, EAF*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [MET], the TSF shall [selection: *REBOOT, PROGRESSIVELY LENGTHEN THE TIME TO ATTEMPT AN AUTHENTICATION, MAKE ALL USER DATA ASSETS UNREADABLE, [assignment: list of other actions TO REDUCE THE RISK OF ATTACKS SUCH AS BRUTE-FORCE ATTACK]*].

8.3 TOE Security functional requirements

8.3.1 Biometric requirements

8.3.1.1 Identification and Authentication (FIA)

FIA_MBE_EXT.1 Biometric enrolment

FIA_MBE_EXT.1.1 The TSF shall provide a mechanism to enrol an authenticated user to the biometric system.

Application Note 3: User shall be authenticated by the mobile device using the KAF or EAF before beginning biometric enrolment.

FIA_MBV_EXT.1 Biometric verification

FIA_MBV_EXT.1.1 The TSF shall provide a biometric verification mechanism using [selection: FINGERPRINT, *2D FACE, 3D FACE*].

FIA_MBV_EXT.1.2 The TSF shall provide a biometric verification mechanism with the [FAR] not exceeding [~~assignment:~~ selection: *1:50 000 FOR 2D FACE, 1:100 000 FOR 3D FACE, 1:50 000 FOR FINGERPRINT*] and [FRR] not exceeding [~~assignment:~~ selection: *1:20 FOR 2D FACE, 1:33 FOR 3D FACE, 1:33 FOR FINGERPRINT*].

Application Note 4: If the TOE supports multiple modalities, the ST author may iterate the SFR to define different error rates for each modality.

8.3.1.2 Security Management (FMT)

FMT_SMF.1/BAF Specification of Management Functions

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

- *ENROL THE INITIAL [selection: 2D FACE, 3D FACE, FINGERPRINT]; AND*
- *RE-ENROL OR CHANGE THE [selection: 2D FACE, 3D FACE, FINGERPRINT]*.

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.AUTHENTICATE_USER (from Base-PP)	This objective is achieved (in the PP-Module) by FIA_AFL.1 (modified), FIA_UAU.5/Local (modified) and FIA_MBV_EXT.1 by adding biometric verification to the allowed authentication methods.
O.BIO_VERIFICATION	This objective is achieved by FIA_MBV_EXT.1 that verifies a user's biometric, to identify the user.
O.ENROL	This objective is achieved by: • FIA_MBE_EXT.1 enrols an already authenticated user. • FMT_SMF.1/BAF provides the user with the ability to manage their biometric credentials.

8.4.3 Dependency analysis

SFR	Dependency	Rationale
FIA_AFL.1	FIA_UAU.1	Fulfilled by FIA_UAU.1 in Base-PP
FIA_MBE_EXT.1	-	
FIA_MBV_EXT.1	FIA_MBE_EXT.1	Fulfilled by FIA_MBE_EXT.1
FIA_UAU.5/Local	-	
FMT_SMF.1/BAF	-	

8.5 Consistency rationale

8.5.1 TOE type consistency

When this PP-Module is used to extend the ETSI TS 103 732-1 [5] Base-PP, the TOE type for the overall TOE is still a generic mobile device. However, one of the functions of the device shall be the ability for it to have biometric enrolment and verification capability. The TSF boundary is simply extended to include that functionality.

8.5.2 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 [5] base-PP as follows:

PP-Module Threats	Consistency Rationale
T.BIO_IMPERSONATE	The threat of zero-effort imposter attempts are specific subsets of the T.PHYSICAL (i.e. impersonate the user authentication mechanisms) threat in the ETSI TS 103 732-1 [5].
P.VERIFICATION	
P.ENROL	

8.5.3 Consistency of Objectives

The objectives for the biometric system and its operational environment are consistent with the ETSI TS 103 732-1 [5] Base-PP based on the following rationale:

PP-Module TOE Objectives	Consistency Rationale
O.BIO_VERIFICATION	These TOE Objectives are specific subsets of the O.AUTHENTICATE_USER objective in the ETSI TS 103 732-1 [5].
O.ENROL	

8.5.4 Consistency of Requirements

The biometric system (i.e. TOE in this PP-Module) is comprised of biometric capture sensors and firmware/software that provide functions described in clause 4.2. The biometric system is invoked by the mobile device as defined in the ETSI TS 103 732-1 [5] when user's biometric characteristics are presented to the sensor. The biometric system creates and stores the template or compares the features with the stored template and returns the verification outcome to the mobile device.

This PP-Module assumes that the mobile device satisfies SFRs defined in the ETSI TS 103 732-1 [5] so that the biometric system can work as specified in this PP-Module. There are no specific SFR selections from ETSI TS 103 732-1 [5] that are required by the PP-Module. As the requirements in the PP-Module are additional to the ETSI TS 103 732-1 [5] requirements, there is no contradiction between the two sets of requirements.

For any modality selected in the updated FIA_UAU.5/Local, the mobile device shall invoke the biometric system to unlock the device under the conditions specified in the updated FIA_AFL.1 requirement. The mobile device shall follow the rule(s) laid out in FIA_UAU.5.2/Local for determining the method for user authentication.

The biometric system shall implement a verification mechanism that satisfies the SFRs defined in this PP-Module, where matching modalities shall be specified in FIA_UAU.5/Local, FIA_AFL.1 and FIA_MBV_EXT.1. Iterations of FIA_MBV_EXT.1 are allowed to make it easier to clearly specify the claims for each modality.

Annex A (informative): Bibliography

- CCMB-2017-04-004 Version 3.1 revision 5, April 2017: "Common Methodology for Information Technology Security Evaluation: Evaluation methodology".
- ETSI EN 303 645 (V2.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".
- ISO/IEC 30107-4:2020: "Information Technology - Biometric Presentation Attack Detection - Part 4: Profile for testing of mobile devices".
- Biometrics Security iTC: "Collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module]", version 1.1, September 12, 2022.

History

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