collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device -

Version 0.8, 2019-06-13

Table of Contents

1. Acknowledgements

This collaborative PP-Module was developed by the Biometrics Security international Technical Community (BIO-iTC) with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

2. Preface

2.1. Objectives of Document

This document presents the Common Criteria (CC) collaborative PP-Module to express the security functional requirements (SFRs) and security assurance requirements (SARs) for mobile biometric enrolment and verification on the mobile device. The Evaluation activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this PP-Module, are described in [SD].

2.2. Scope of Document

The scope of the PP-Module within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation. In particular, a PP-Module defines the IT security requirements of a generic type of TOE and specifies the functional security measures to be offered by that TOE to meet stated requirements [CC1], Section B.14.

2.3. Intended Readership

The target audiences of this PP-Module are developers, CC consumers, system integrators, evaluators and schemes.

Although the PP-Module and [SD] may contain minor editorial errors, the PP-Module is recognized as living document and the iTC is dedicated to ongoing updates and revisions. Please report any issues to the BIO-iTC.

2.4. Related Documents

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017.
- [addenda] CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, May 2017.

- [SD] Evaluation Activities for collaborative Protection Profile Module for Mobile biometric enrolment and verification - for unlocking the device -, January-2019, Version 0.3.
- [ISO/IEC 19795-1] Biometric performance testing and reporting — Part 1: Principles and framework, First edition.
- [ISO/IEC 19989-2] Information technology - Security techniques - Criteria and methodology for security evaluation of biometric systems - Part 2: Biometric recognition performance
- [ISO/IEC 19989-3] Information technology - Security techniques - Criteria and methodology for security evaluation of biometric systems - Part 3: Presentation attack detection
- [ISO/IEC 21879] Performance testing of biometrics on mobile devices
- [ISO/IEC 29156] Information technology - Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics, 2015.
- [ISO/IEC 30107-1] Biometric presentation attack detection - Part 1: Framework, First edition.
- [ISO/IEC 30107-3] Biometric presentation attack detection - Part 3: Testing and reporting, First edition.
- [ISO/IEC 30107-4] Information technology - Biometric presentation attack detection - Part 4: Profile for testing of mobile devices
- [MDFPP] Protection Profile for Mobile Device Fundamentals, Version:3.2
- [NIST800-63B] NIST Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management, June 2017

2.5. Glossary

For the purpose of this PP-Module, the following terms and definitions given in ISO/IEC 19795-1, ISO/IEC 30107-1 and [MDFPP] apply. If the same terms and definitions are given in those references, terms and definitions that fit the context of this PP-Module take precedence. Some terms and definitions are also adjusted to match the context of the mobile biometric enrolment and verification.

Attempt

Submission of one (or a sequence of) biometric samples to the part of the TOE.

Biometric Authentication Factor (BAF)

Authentication factor used for mobile biometric verification. In this PP-Module, the term is a synonym of the “template”.

Biometric Data

Digital data created during biometric enrolment and verification processes. It encompasses raw sensor observations, biometric samples, features, templates, and/or similarity scores, among other data. This data is used to describe the information collected, and does not include end user information such as user name, password (unless tied to the biometric modality), demographic information, and authorizations.

Biometric System Administrator

Person who is responsible for configuring the TOE. This PP-Module assumes that the user acts as

the biometric system administrator.

Failure-To-Enroll Rate (FTE)

Proportion of the population for whom the system fails to complete the enrolment process.

False Accept Rate (FAR)

Proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.

False Match Rate (FMR)

Proportion of zero-effort impostor attempt samples that were falsely declared to match the compared non-self template.

False Non-match Rate (FNMR)

Proportion of genuine attempt samples that were falsely declared not to match the template of the same characteristic from the same user supplying the sample.

False Reject Rate (FRR)

Proportion of verification transactions with truthful claims of identity that are incorrectly denied.

Features

Digital representation of the information extracted from a sample (by the signal processing subsystem) that will be used to construct or compare against enrolment templates.

Hybrid Authentication

A hybrid authentication factor is one where a user has to submit a combination of biometric sample and PIN or password with both to pass and without the user being made aware of which factor failed, if either fails.

Locked State

Powered on Mobile Device, with most functionalities unavailable for use. User authentication is required to access full functionality.

Mobile Device

A device which is composed of a hardware platform and its system software. The device typically provides wireless connectivity and may include software for functions like secure messaging, email, web, VPN connection, and VoIP (Voice over IP), for access to the protected enterprise network, enterprise data and applications, and for communicating to other Mobile Devices.

Mobile Device User (User)

The individual authorized to physically control and operate the Mobile Device. This PP-Module assumes that the user is the device owner.

(Biometric) Modality

A type or class of biometric system, such as fingerprint recognition, facial recognition, iris recognition, voice recognition, signature/sign, and others.

Password Authentication Factor

A type of authentication factor requiring the user to provide a secret set of characters to gain access.

Presentation Attack

Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.

Presentation Attack Detection (PAD)

Automated determination of a presentation attack.

Presentation Attack Instrument (PAI)

Biometric characteristic or object used in a presentation attack (e.g. artificial or abnormal biometric characteristics). Accompanying [SD] specifies PAIs that the evaluator should consider for the CC evaluation.

(Biometric) Sample

User's biometric measures as output by the data capture subsystem of the TOE.

Secure Execution Environment

An operating environment separate from the main Mobile Device operating system. Access to this environment is highly restricted and may be made available through special processor modes, separate security processors or a combination to provide this separation.

Similarity score

Measure of the similarity between features derived from a sample and a stored template, or a measure of how well these features fit a user's reference model.

Template

User's stored reference measure based on features extracted from enrolment samples.

Transaction

Sequence of attempts on the part of a user for the purposes of an enrolment and verification.

Zero-effort Impostor Attempt

Attempt in which an individual submits his/her own biometric characteristics as if he/she were attempting successful verification against his/her own template, but the comparison is made against the template of another user.

2.6. Revision History

Table 1. Revision history

Version	Date	Description
0.1	24th Oct, 2017	Preliminary draft for the Berlin iTC session
0.2	26th Feb, 2018	First version uploaded to the repo in the Github for review

Version	Date	Description
0.3	9th Mar, 2018	Add SFRs and make editorial changes
0.6	13th Jul, 2018	Add ECDs and make editorial changes
0.8	1st May, 2019	Convert the cPP as of 11th Jan, 2019 into the PP-Module

3. PP Introduction

3.1. PP Reference Identification

- PP Reference: collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device -
- PP Version: 0.8
- PP Date: 2019-06-13

3.2. TOE Overview

This is a collaborative Protection Profile Module (PP-Module) that is used to extend the base PP (Protection Profile for Mobile Device Fundamentals [MDFPP]) for the mobile device that implement mobile biometric enrolment and verification to unlock the mobile device in the locked state using user's biometric characteristics. Therefore, the Target of Evaluation (TOE) in this PP-Module is a mobile device that implements mobile biometric enrolment and verification functionality. However, the term TOE in this document expresses the biometric system that is a part of the TOE (i.e. mobile device) and implements the mobile biometric enrolment and verification functionality for clearly describing the relation and boundary between the biometric system and mobile device. Each mobile biometric enrolment and verification process is described in the following paragraphs.

a) Mobile biometric enrolment

During the enrolment process, the TOE captures samples from the biometric characteristics of a user presented to the TOE and extracts the features from the samples. The features are then stored as a template in the TOE.

Only a user who knows the mobile device password can enrol or revoke his/her own templates. Multiple templates may be enrolled, as separate entries uniquely identified by the TOE, and optionally uniquely identifiable by the user (through the mobile User Interface).

b) Mobile biometric verification

During the verification process, a user presents his/her own biometric characteristics to the TOE without presenting any user identity information for unlocking the mobile device. The TOE captures samples from the biometric characteristics, retrieves all enrolled templates and compares them with the features extracted from the captured samples of the user to measure the similarity between the two data and determines whether to accept or reject the user based on the similarity,

and indicates the decision to the mobile device.

Examples of biometric characteristic used by the TOE are: fingerprint, face, iris, palm print, finger vein, palm vein, speech, signature and so forth. However, scope of this PP-Module is limited to only those biometric characteristics for which [SD] defines the Evaluation Activities.

c) Presentation Attack Detection (PAD)

The TOE needs to consider the risk of subverting the TOE's biometric verification. Attacker could present artificial PAIs to the TOE to interfere with the TOE's security objectives. The TOE needs to be able to provide resistance to presentation attacks. [SD] explains what resistance should be provided by the TOE in detail.

3.3. TOE Design

The TOE is fully integrated into the mobile device without the need for additional software and hardware. The following figure, inspired from ISO/IEC 30107-1, is a generic representation of a TOE. It should be noted that the actual TOE design may not directly correspond to this figure and the developer may design the TOE in a different way. This illustrates the different sub-functionalities on which the mobile biometric enrolment and verification processes rely on.

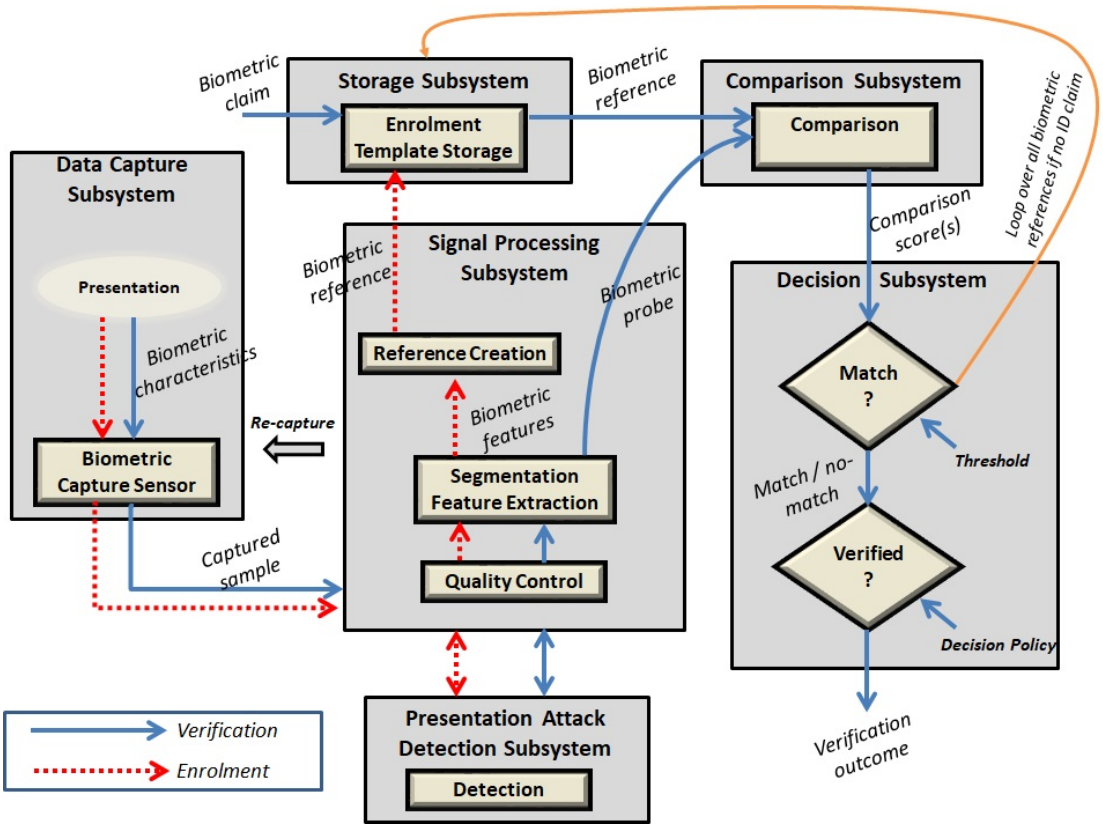

Figure 1. Generic representation of a TOE

As illustrated in the above figure, the TOE is capable of:

- Capturing samples from user's biometric characteristics (Data Capture Subsystem)
- Extracting and processing the features from samples of sufficient quality and generating various templates (Signal Processing Subsystem)

- Storing the templates in a database on the mobile device (Data Storage Subsystem)
- Comparing captured features with data contained in one or more templates (Comparison Subsystem)
- Detecting the presentation attacks using artificial PAI (Presentation Attack Detection Subsystem)
- Deciding how well features and any template match, and indicating whether or not a verification of the user has been achieved (Decision Subsystem)

3.4. Relation between TOE and mobile device

The TOE is reliant on the mobile device itself to provide overall security of the system. This PP-Module is intended to be used with [MDFPP], and [MDFPP] is responsible for evaluating the following security functions:

- Providing the Password Authentication Factor to support user authentication and management of the TOE security function
- Invoking the TOE to enrol and verify the user and take appropriate actions based on the decision of the TOE
- Providing the secure execution environment that guarantees the TOE and its data to be protected with respect to confidentiality and integrity

The evaluation of the above security functions is out of scope of this PP-Module and expected to be performed separately based on the [MDFPP]. Relation between this PP-Module and [MDFPP] is explained in detail in Annex A Consistency Rationale between this PP-Module and MDFPP.

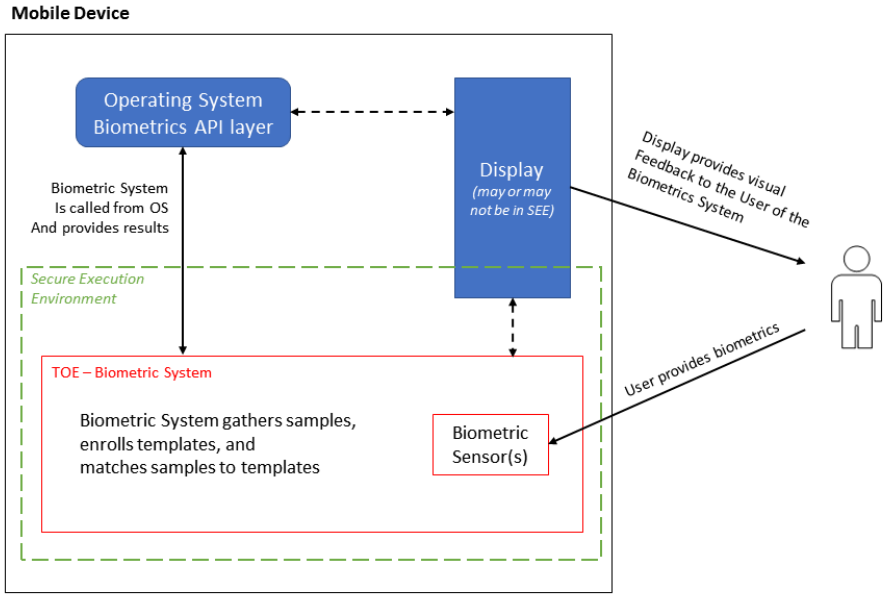

Figure 2. Generic relations between the TOE and the mobile device environment

3.5. TOE Use Case

Mobile device itself may be operated in a number of use cases such as enterprise use with limited personal use or Bring Your Own Device (BYOD). The TOE on the device may also be operated in the same use cases, however, use cases of the TOE should be devised separately considering the purpose of mobile biometric verification and potential attacks. The following use cases describe how and why mobile biometric verification is supposed to be used. Each use case has its own assurance level, depending on its criticality and separate PP or PP-Module should be developed for each use case.

This PP-Module only assumes USE CASE 1 described below. USE CASE 2 is out of scope of this PP-Module.

3.5.1. USE CASE 1: Mobile biometric verification for unlocking the mobile device

For enhanced security that is easy to use, mobile device may implement mobile biometric verification on a device once it has been “unlocked”. The initial unlock is generally done by a PIN/password which is required at startup (or possibly after some period of time), and after that the user is able to use an own biometric characteristic to unlock access to the mobile device. In this use case, the mobile device is not supposed to be used for security sensitive services through the mobile biometric verification.

Main concern of this use case is the accuracy of mobile biometric verification (i.e. FAR/FMR and FRR/FNMR) and basic level of presentation attacks. Security assurance for mobile device that the TOE relies on should be handled by [MDFPP].

This use case assumes that the mobile device is configured correctly to enable the mobile biometric verification by the biometric system administrator. The user of the mobile device can act as the biometric system administrator in this use case.

It is also assumed that the user enrols his/herself correctly, following the guidance provided by the TOE. Attacks during enrolment may be out of scope, but optionally addressed. FTE is not a security relevant criterion for this use case.

3.5.2. USE CASE 2: Mobile biometric verification for security sensitive service

This use case is an example of another use case that isn’t considered in this PP-Module. Another PP-Module should be developed at higher assurance level for this use case.

Mobile devices may be used for security sensitive services such as payment transactions and online banking. Verification may be done by the biometric for convenience instead of PIN/password to access such security sensitive services.

The requirements for the TOE focus on the biometric performance (FTE, FAR/FMR and FRR/FNMR) and higher level of presentation attack.

4. CC Conformance Claims

As defined by the references [CC1], [CC2] and [CC3], this PP-Module:

- conforms to the requirements of Common Criteria v3.1, Revision 5,
- is Part 2 extended,
- does not claim conformance to any other security functional requirement packages.

In order to be conformant to this PP-Module, a ST shall demonstrate Exact Conformance. Exact Conformance, as a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the SFRs in Security Functional Requirements (these are the mandatory SFRs) of this PP-Module, and potentially SFRs from Selection-Based Requirements (these are selection-based SFRs) and Optional Requirements (these are optional SFRs) of this PP-Module. While iteration is allowed, no additional requirements (from [CC2] or [CC3], or definitions of extended components not already included in this PP-Module) are allowed to be included in the ST. Further, no SFRs in Security Functional Requirements of this PP-Module are allowed to be omitted.

5. Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

This PP-Module is written to address the situation described in the section USE CASE 1: Mobile biometric verification for unlocking the mobile device.

Note that as a PP-Module, all threats, assumptions, and OSPs defined in [MDFPP] will also apply to a TOE unless otherwise specified. The SFRs defined in this PP-Module will mitigate the threats that are defined in the PP-Module but may also mitigate some threats defined in the [MDFPP] in more comprehensive detail due to the specific capabilities provided by a biometric system.

5.1. Threats

T.Casual_Attack

An attacker may attempt to impersonate as a legitimate user without being enrolled in the TOE. In order to perform the attack, the attacker only use his/her own biometric characteristic (in form of a zero-effort impostor attempt).

T.Presentation_Attack

An attacker may attempt a presentation attack to the TOE. In order to perform the attack, the attacker uses artificial Presentation Attack Instrument (PAI) except his/her own biometric characteristic.

5.2. Organizational Security Policies

OSP.Enrol

The TOE shall enrol a user for mobile biometric verification, only after successful authentication of a user. The TOE shall ensure that templates are of sufficient quality in order to meet the relevant error rates for mobile biometric verification.

OSP.PAD_Error

The TOE shall meet relevant criteria for its security relevant error rates for PAD.

OSP.Protection

The TOE in cooperation with its environment shall protect itself, its configuration and biometric data.

OSP.Verification_Error

The TOE shall meet relevant criteria for its security relevant error rates for mobile biometric verification.

5.3. Assumptions

A.Alternative

It is assumed that the TOE environment provides an alternative authentication mechanism as a complement to mobile biometric verification. The alternative authentication mechanism is required for enrolment of the biometric template and can also be used in cases when a user is rejected by the mobile biometric verification (False Rejection).

A.Authentication

It is assumed that the TOE environment invokes the TOE for mobile biometric verification, and take appropriate actions based on the TOE's decision.

A.User

It is assumed that the user configures the TOE and its environment correctly in a manner to ensure that the TOE security policies will be enforced.

6. Security Objectives

This PP-Module defines the following security objectives beyond those specified in [MDFPP].

6.1. Security Objectives for the TOE

O.BIO_Verification

The TOE shall provide a mobile biometric verification mechanism to verify a user with an adequate reliability. The TOE shall meet the relevant criteria for its security relevant error rates for mobile biometric verification.

SFR Rationale:

Requirements to provide a mobile biometric verification mechanism is defined in FIA_MBV_EXT.1

in which ST author can specify the relevant criteria for its security relevant error rates. FIA_MBV_EXT.2 requires the TOE to only use samples of sufficient quality to verify a user with an adequate reliability.

Application Note 1

In this PP-Module, relevant criteria are FAR/FMR and FRR/FNMR and corresponding error rates shall be specified in the FIA_MBV_EXT.1.

O.Enrol

The TOE shall implement the functionality to enrol a user for mobile biometric verification and bind the template to the user only after successful authentication of the user to the TOE environment using an alternative authentication mechanism. The TOE shall create the sufficient quality of templates in order to meet the relevant error rates for mobile biometric verification.

SFR Rationale:

Requirements to provide a mobile biometric enrolment mechanism is defined in FIA_MBE_EXT.1. Requirement for quality of template is defined in FIA_MBE_EXT.2.

Application Note 1

A user shall be authenticated using a Password Authentication Factor to enrol his/herself as required by [MDFPP].

Application Note 2

In this PP-Module, relevant criteria are FAR/FMR and FRR/FNMR and corresponding error rates shall be specified in the FIA_MBV_EXT.1.

O.Presentation_Attack_Detection

The TOE shall prevent a presentation attack using artificial PAIs. The TOE shall meet relevant criteria for its security relevant error rates for PAD.

SFR Rationale:

Requirement to provide a presentation attack detection mechanism during mobile biometric verification is defined in FIA_MBV_EXT.3. [SD] defines relevant criteria for its security relevant error rates for PAD in the Evaluation Activity for FIA_MBV_EXT.3. Optional requirement to provide a presentation attack detection mechanism during mobile biometric enrolment is defined as FIA_MBE_EXT.3.

Application Note 3

The TOE may or may not counter a presentation attack during enrolment. If the ST author requires the TOE to counter the presentation attack during enrolment, ST author should include FIA_MBE_EXT.3 defined in Optional Requirements.

Application Note 4

According to the ISO/IEC 30107-3, relevant error rates should be specified for each type of PAI. [SD] defines PAIs that should be used for attack and describes how to create and present the PAIs to the TOE, and minimum error rates that the TOE shall achieve.

O.Protection

The TOE shall protect biometric data using the secure execution environment provided by the TOE environment.

SFR Rationale:

Requirements to control access to the template is defined in FPT_PBT_EXT.1. FPT_BDP_EXT.1, FPT_BDP_EXT.2 and FPT_BDP_EXT.3 requires the TOE to protect the biometric data with support from the TOE environment. Optional requirements to protect the residual biometric data is defined as FDP_RIP.2 in Optional Requirements.

Application Note 5

As described in Annex A Consistency Rationale between this PP-Module and MDFPP, the TOE and TOE environment (i.e. mobile device) shall satisfy relevant requirements defined in this PP-Module and [MDFPP] respectively to protect biometric data.

6.2. Security Objectives for the Operational Environment

OE.Alternative

The TOE environment shall provide an alternative authentication mechanism as a complement to mobile biometric verification. The alternative authentication mechanism is required for enrolment of the biometric template and can also be used in cases where a user is rejected by the mobile biometric verification (False Rejection).

Application Note 6

As described in Annex A Consistency Rationale between this PP-Module and MDFPP, the TOE environment (i.e. mobile device) shall satisfy relevant requirements defined in [MDFPP].

Application Note 7

Alternative authentication mechanism shall use the Password Authentication Factor as required by [MDFPP].

OE.Authentication

The TOE environment shall invoke the TOE for mobile biometric verification, and take appropriate actions based on the TOE's decision.

Application Note 8

As described in Annex A Consistency Rationale between this PP-Module and MDFPP, the TOE environment (i.e. mobile device) shall satisfy relevant requirements defined in [MDFPP].

Application Note 9

Appropriate actions taken by the mobile device are unlocking the mobile device or incrementing the number of unsuccessful attempts and limiting maximum number of unsuccessful attempts.

OE.Protection

The TOE environment shall provide a secure execution environment to protect the TOE, the TOE

configuration and biometric data during runtime and storage.

Application Note 10

As described in Annex A Consistency Rationale between this PP-Module and MDFPP, the TOE and TOE environment (i.e. mobile device) shall satisfy related requirements defined in this PP-Module and [MDFPP] respectively.

OE.User

The user shall configure the TOE and its environment correctly in a manner to ensure that the TOE security policies will be enforced.

Application Note 11

Mobile device shall be configured by the user as required by [MDFPP].

6.3. Security Objectives Rationale

The following table describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 2. Mapping between Security Problem Defintion and Security Objectives

Threat, Assumption, or OSP	Security Objectives	Rationale
T.Casual_Attack OSP.Verification_Error	O.BIO_Verification	The threat T.Casual_Attack is countered by O.BIO_Verification as this provides the capability of mobile biometric verification not to allow the user who have not been enrolled to impersonate as a legitimate user. The OSP OSP.Verification_Error is enforced by O.BIO_Verification as this requires the TOE to meet relevant criteria for security relevant error rates for mobile biometric verification.
OSP.Enrol	O.Enrol	The OSP OSP.Enrol is enforced by O.Enrol as this require the TOE to implement the functionality to enrol a user for mobile biometric verification and create sufficient quality of templates.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.Presentation_Attack OSP.PAD_Error	O.Presentation_Attack_Detection	The threat T.Presentation_Attack is countered by O.Presentation_Attack_Detection as this provides the capability of mobile biometric verification to prevent attacks with artificial PAIs. The OSP OSP.PAD_Error is enforced by O.Presentation_Attack_Detection as this requires the TOE to meet relevant criteria for security relevant error rates for PAD.
OSP.Protection	O.Protection OE.Protection	The OSP OSP.Protection is enforced by O.Protection and its operational environment objective OE.Protection.
A.Alternative	OE.Alternative	The Assumption A.Alternative is satisfied by the operational environment objective OE.Alternative.
A.Authentication	OE.Authentication	The Assumption A.Authentication is satisfied by the operational environment objective OE.Authentication.
A.User	OE.User	The Assumption A.User is satisfied by the operational environment objective OE.User.

7. Security Functional Requirements

7.1. MDFPP Security Functional Requirements Direction

This section instructs the ST author on what selections must be made to certain SFRs contained in the [MDFPP] in order to mitigate a threat from the [MDFPP] in a more specific or restrictive manner as described in this PP-Module than specified in the [MDFPP].

FIA_UAU.5 Multiple Authentication Mechanisms

There is no change to the text of this SFR. However; the ST author must select at least one modality in FIA_UAU.5.1. The ST author shall select the same modality in FIA_MBV_EXT.1.1 in this PP-Module.

7.2. Conventions

The individual security functional requirements are specified in the sections below. The following conventions are used for the completion of operations:

- [*Italicized text within square brackets*] indicates an operation to be completed by the ST author.
- **Bold text** indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [text within square brackets] indicates the completion of a selection.
- Number in parentheses after SFR name, e.g. (1) indicates the completion of an iteration.

Extended SFRs are identified by having a label “EXT” at the end of the SFR name.

7.3. Identification and Authentication (FIA)

7.3.1. FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBE_EXT.1.1

The TSF shall provide a mechanism to enrol an authenticated user.

Application Note 12

User shall be authenticated by the mobile device using the Password Authentication Factor before beginning biometric enrolment.

7.3.2. FIA_MBE_EXT.2 Quality of biometric templates for mobile biometric enrolment

FIA_MBE_EXT.2.1 The TSF shall create templates of sufficient quality.

Application Note 13

ST author may refine “sufficient quality” to specify quality standards if the TOE follows such standard.

7.3.3. FIA_MBV_EXT.1 Mobile biometric verification

FIA_MBV_EXT.1.1

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

FIA_MBV_EXT.1.2

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

Application Note 14

If the TOE support multiple modalities, ST author may iterate the SFR to define different error

rates for each modality.

Application Note 15

ST author shall select or assign those modalities in FIA_MBV_EXT.1.1 for which [SD] defines the Evaluation Activities.

Application Note 16

Value of FMR, FAR, FNMR and FRR shall be assigned by the ST author however the ST author should consider the following factors for setting those values.

a) Allowed maximum values defined in the standards

For example, [NIST800-63B] requires that FMR shall be 1 in 1000 or lower. ISO/IEC 29156 suggests as a simple rule of thumb that for basic, medium and high levels of authentication assurance, rates of 1% (1 in 100), 0.01% (1 in 10^4) and 0.0001% (1 in 10^6) can be considered as suitable target figures for FAR". Several mobile vendors have specified fingerprint verification shall have the FAR lower than 0.002% and recommended to have the FRR lower than 10%. The PP-Module doesn't provide any recommendation for those error rates however, ST author should set appropriate error rates referring those value.

For consistency in language throughout this document, referring to a "lower" number will mean the chance of occurrence is lower (i.e. 1/100 is lower than 1/20). So, saying device 1 has a lower FAR than device 2 means device 1 could have 1/1000 and device 2 would be 1/999 or higher in terms of likelihood. Saying "greater" will explicitly mean the opposite.

b) Technical limitation

Although different modalities are available for the mobile biometric verification, all modalities may not achieve the same level of accuracy. For modalities that have different target of error rates, ST author may iterate the requirement to set appropriate error rates for each modality.

c) Number of test subjects required for the performance testing

Target error rates defined in SFR shall be evaluated based on [SD]. Normally the target error rates will directly influence the size of the test subject, the time and cost of the testing. [SD] describes how those error rates should be evaluated in an objective manner.

7.3.4. FIA_MBV_EXT.2 Quality of biometric samples for mobile biometric verification

FIA_MBV_EXT.2.1 The TSF shall only use samples of sufficient quality to verify the user.

Application Note 17

ST author may refine "sufficient quality" to specify quality standards if the TOE follows such standard.

7.3.5. FIA_MBV_EXT.3 Presentation attack detection for mobile biometric verification

FIA_MBV_EXT.3.1 The TSF shall prevent use of artificial presentation attack instruments from being successfully verified.

Application Note 18

This requirement is only applicable to mobile biometric verification. PAD for mobile biometric enrolment is an optional requirement.

Application Note 19

Artificial PAIs that the TOE shall prevent and relevant criteria for its security relevant error rates for each type of PAI is defined in [SD].

7.4. Protection of the TSF (FPT)

7.4.1. FPT_BDP_EXT.1 Biometric data processing

FPT_BDP_EXT.1.1 The TSF shall process any plaintext biometric data used to generate templates and perform sample matching within the security boundary of the secure execution environment.

Application Note 20

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

7.4.2. FPT_BDP_EXT.2 No Biometric data transmission

FPT_BDP_EXT.2.1 The TSF shall not transmit any plaintext biometric data outside the security boundary of the secure execution environment.

Application Note 21

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

7.4.3. FPT_BDP_EXT.3 Biometric data storage

FPT_BDP_EXT.3.1 The TSF shall not store any plaintext biometric data outside the security boundary of the secure execution environment.

Application Note 22

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

7.4.4. FPT_PBT_EXT.1 Protection of biometric template

FPT_PBT_EXT.1.1

The TSF shall protect the template [**selection**: *using a PIN as an additional factor, using a password as an additional factor*, [**assignment**: *other circumstances*]].

Application Note 23

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

8. Security Assurance Requirements

This PP-Module does not define any additional assurance requirements above and beyond what is defined in the [MDFPP] 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.

9. Consistency Rationale

9.1. Protection Profile for Mobile Device Fundamentals

9.1.1. Consistency of TOE Type

If this PP-Module is used to extend [MDFPP], the TOE type for the overall TOE is still a generic mobile device. However, one of the functions of the device must be the ability for it to have biometric enrolment and verification capability. The TOE boundary is simply extended to include that functionality.

9.1.2. Consistency of Security Problem Definition

The threats, OSPs and assumptions defined by this PP-Module (see Section Threats, Organizational Security Policies and Assumptions) are consistent with those defined in the [MDFPP] as follows:

Table 3. Consistency Rationale for threats and OSPs

PP-Module Threats/OSPs	Consistency Rationale
T.Casual_Attack	The threat of zero-effort impostor attempt and presentation attack with related OSPs are specific subsets of the [T.PHYSICAL] (i.e. impersonate the user authentication mechanisms) threat in the [MDFPP].
T.Presentation_Attack	
OSP.Enrol	
OSP.PAD_Error	
OSP.Verification_Error	
OSP.Protection	This OSP is specific subsets of the [T.PHYSICAL] (i.e. direct and possibly destructive access to its storage media (biometric data)) threat in the [MDFPP].

Table 4. Consistency Rationale for Assumptions

PP-Module Assumptions	Consistency Rationale
A.Alternative	All assumptions levied on the operational environment of biometric system (i.e. mobile device) are consistent with security requirements in the [MDFPP]. See Annex A Consistency Rationale between this PP-Module and MDFPP.
A.Authentication	
A.User	

9.1.3. Consistency of Objectives

The objectives for the biometric system and its operational environment are consistent with the [MDFPP] based on the following rationale:

Table 5. Consistency Rationale for TOE Objectives

PP-Module TOE Objectives	Consistency Rationale
O.BIO_Verification	These TOE Objectives are specific subsets of the [O.AUTH] objective in the [MDFPP].
O.Enrol	
O.Presentation_Attack_Detection	
O.Protection	This TOE Objective is specific subset of the [O.STORAGE] objective in the [MDFPP].

Table 6. Consistency Rationale for Environmental Objectives

PP-Module Environmental Objectives	Consistency Rationale
OE.Alternative	All Environmental Objectives levied on the operational environment of biometric system (i.e. mobile device) are consistent with security requirements in the [MDFPP]. See Annex A Consistency Rationale between this PP-Module and MDFPP
OE.Authentication	
OE.Protection	
OE.User	

9.1.4. Consistency of Requirements

This PP-Module identifies several SFRs from [MDFPP] that are needed to support biometric system functionality. The rationale for why this does not conflict with the claims defined by the [MDFPP] are described in Annex A Consistency Rationale between this PP-Module and MDFPP

10. Selection-Based Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that shal be performed by the TOE) are contained in Security Functional Requirements. Additionally, there are two other types of requirements specified in Selection-Based Requirements and Optional Requirements.

The first type (in this Section) comprises requirements based on selections in other SFRs from the PP-Module: if certain selections are made, then additional requirements in this Section will need to be included in the body of the ST.

The second type (in Section Optional Requirements) comprises requirements that can be included in the ST, but are not mandatory for a TOE to claim conformance to this PP-Module.

10.1. Identification and Authentication (FIA)

The following SFR shall be used by the ST author if 'hybrid' is selected in FIA_UAU.5.1.

10.1.1. FIA_HYB_EXT.1 Hybrid Authentication Biometric Method

FIA_HYB_EXT.1.1 The TOE shall only use [**selection**: *fingerprint, iris, face, voice, vein*], [**assignment:** *other modality*] as the biometric component of the hybrid authentication mechanism.

Application Note 24

A hybrid authentication mechanism is one where a user has to submit a combination of biometric sample and PIN or password with both to pass and without the user being made aware of which factor failed, if either fails. If this mechanism is selected in the [MDFPP], the above component shall also be selected.

11. Optional Requirements

ST authors are free to choose none, some or all SFRs defined in this Section. Just the fact that a product supports a certain functionality does not mandate to add any SFR defined in this chapter.

11.1. Identification and Authentication (FIA)

11.1.1. FIA_MBE_EXT.3 Presentation attack detection for mobile biometric enrolment

FIA_MBE_EXT.3.1 The TSF shall prevent use of artificial presentation attack instruments from being successfully enrolled.

11.2. User data protection (FDP)

11.2.1. FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of biometric data is made unavailable upon the [**selection**: *allocation of the resource to, deallocation of the resource from*] all objects.

Application Note 25

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment protect biometric data in detail.

12. Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module, including those used in Selection-Based Requirements and Optional Requirements.

(Note: formatting conventions for selections and assignments in this Section are those in [CC2].)

12.1. Identification and Authentication (FIA)

12.1.1. Mobile 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

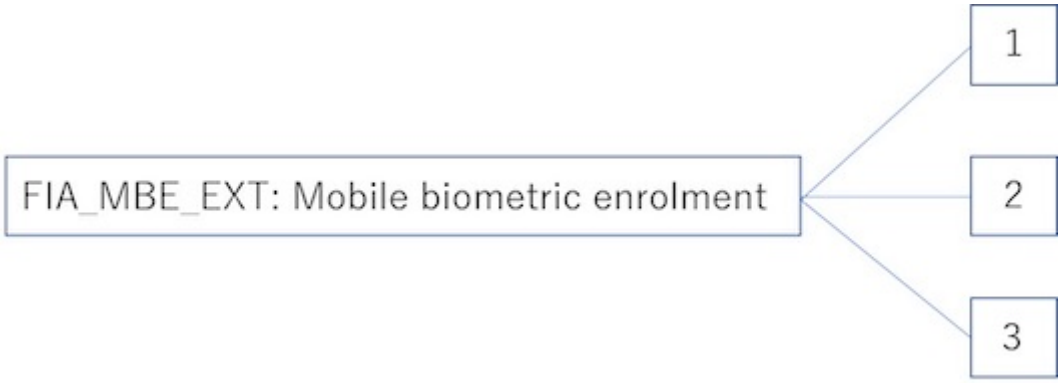

Figure 3. Component levelling

FIA_MBE_EXT.1 Mobile biometric enrolment requires the TSF to enrol a user.

FIA_MBE_EXT.2 Quality of biometric templates for mobile biometric enrolment requires the TSF to create templates of sufficient quality.

FIA_MBE_EXT.3 Presentation attack detection for mobile biometric enrolment requires the TSF to prevent presentation attacks during the mobile biometric enrolment.

Management: FIA_MBE_EXT.1

There are no management activities foreseen.

Management: FIA_MBE_EXT.2

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

a) the management of the TSF data (setting threshold values for quality scores to generate templates) by an administrator.

Management: FIA_MBE_EXT.3

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

a) the management of the TSF data (setting values for detecting artificial presentation attack instruments) by an administrator.

Audit: FIA_MBE_EXT.1, FIA_MBE_EXT.2

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

a) Basic: Success or failure of the mobile biometric enrollment

Audit: FIA_MBE_EXT.3

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

a) Basic: Detection of presentation attacks

FIA_MBE_EXT.1 Mobile 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.

Application Note 26

User shall be authenticated by the mobile device using the Password Authentication Factor before beginning biometric enrolment.

FIA_MBE_EXT.2 Quality of biometric templates for mobile biometric enrolment

Hierarchical to: No other components Dependencies: FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBE_EXT.2.1 The TSF shall create templates of sufficient quality.

Application Note 27

ST author may refine “sufficient quality” to specify quality standards if the TOE follows such standard.

FIA_MBE_EXT.3 Presentation attack detection for mobile biometric enrolment

Hierarchical to: No other components Dependencies: FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBE_EXT.3.1 The TSF shall prevent use of artificial presentation attack instruments from being successfully enrolled.

12.1.2. Mobile biometric verification (FIA_MBV_EXT)

Family Behaviour

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

Component levelling

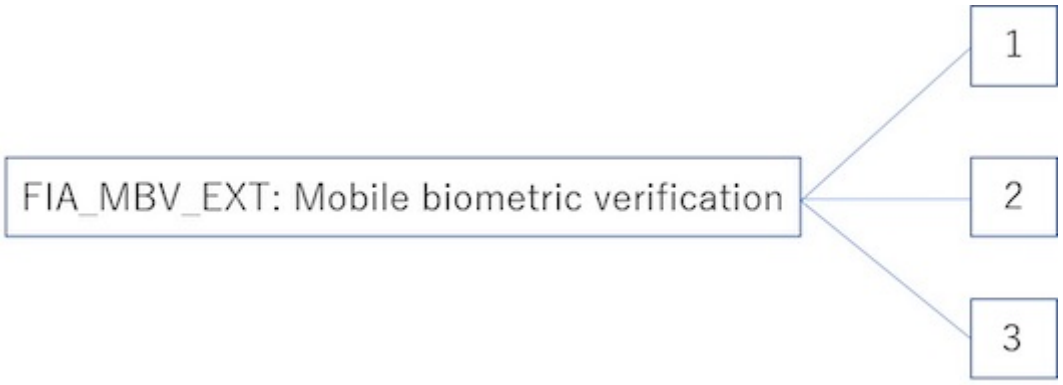

Figure 4. Component levelling

FIA_MBV_EXT.1 Mobile biometric verification requires the TSF to verify a user.

FIA_MBV_EXT.2 Quality of biometric samples for mobile biometric verification requires the TSF to use samples of sufficient quality.

FIA_MBV_EXT.3 Presentation attack detection for mobile biometric verification requires the TSF to prevent presentation attacks during the mobile biometric verification.

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.

Management: FIA_MBV_EXT.2

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

a) the management of the TSF data (setting threshold values for quality scores to check samples) by an administrator.

Management: FIA_MBV_EXT.3

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

a) the management of the TSF data (setting values for detecting artificial presentation attack instruments) by an administrator.

Audit: FIA_MBV_EXT.1, FIA_MBV_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in

the PP/ST:

a) Basic: Success or failure of the mobile biometric verification

Audit: FIA_MBV_EXT.3

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

a) Basic: Detection of presentation attacks

FIA_MBV_EXT.1 Mobile biometric verification

Hierarchical to: No other components

Dependencies: FIA_MBE_EXT.1 Mobile biometric enrolment

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

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

Application Note 28

If the TOE support multiple modalities, ST author may iterate the SFR to define different error rates for each modality.

Application Note 29

ST author shall select or assign those modalities in FIA_MBV_EXT.1.1 for which [SD] defines the Evaluation Activities.

Application Note 30

Value of FMR, FAR, FNMR and FRR shall be assigned by the ST author however the ST author should consider the following factors for setting those values.

a) Allowed maximum values defined in the standards

For example, [NIST800-63B] requires that FMR shall be 1 in 1000 or lower. ISO/IEC 29156 suggests as a simple rule of thumb that for basic, medium and high levels of authentication assurance, rates of 1% (1 in 100), 0.01% (1 in 10^4) and 0.0001% (1 in 10^6) can be considered as suitable target figures for FAR". Several mobile vendors have specified fingerprint verification shall have the FAR lower than 0.002% and recommended to have the FRR lower than 10%. The PP-Module doesn't provide any recommendation for those error rates however, ST author should set appropriate error rates referring those value.

For consistency in language throughout this document, referring to a "lower" number will mean the chance of occurrence is lower (i.e. 1/100 is lower than 1/20). So, saying device 1 has a lower FAR than device 2 means device 1 could have 1/1000 and device 2 would be 1/999 or higher in terms of likelihood. Saying "greater" will explicitly mean the opposite.

b) Technical limitation

Although different modalities are available for the mobile biometric verification, all modalities may not achieve the same level of accuracy. For modalities that have different target of error rates, ST author may iterate the requirement to set appropriate error rates for each modality.

c) Number of test subjects required for the performance testing

Target error rates defined in SFR shall be evaluated based on [SD]. Normally the target error rates will directly influence the size of the test subject, the time and cost of the testing. [SD] describes how those error rates should be evaluated in an objective manner.

FIA_MBV_EXT.2 Quality of biometric samples for mobile biometric verification

Hierarchical to: No other components.

Dependencies:

FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBV_EXT.1 Mobile biometric verification

FIA_MBV_EXT.2.1 The TSF shall only use samples of sufficient quality to verify the user.

Application Note 31

ST author may refine “sufficient quality” to specify quality standards if the TOE follows such standard.

FIA_MBV_EXT.3 Presentation attack detection for mobile biometric verification

Hierarchical to: No other components

Dependencies:

FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBV_EXT.1 Mobile biometric verification

FIA_MBV_EXT.3.1 The TSF shall prevent use of artificial presentation attack instruments from being successfully verified.

Application Note 32

This requirement is only applicable to mobile biometric verification. PAD for mobile biometric enrolment is an optional requirement.

Application Note 33

Artificial PAIs that the TOE shall prevent and relevant criteria for its security relevant error rates for each type of PAI is defined in [SD].

12.1.3. Hybrid Authentication Biometric Method (FIA_HYB_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to verify a user with the hybrid authentication.

Component leveling

Figure 5. Component levelling

FIA_HYB_EXT.1 Hybrid Authentication Biometric Method requires the TSF to verify a user with the hybrid authentication.

Management: FIA_HYB_EXT.1

There are no management activities foreseen.

Audit: FIA_HYB_EXT.1

There are no auditable events foreseen.

FIA_HYB_EXT.1 Hybrid Authentication Biometric Method

Hierarchical to: No other components

Dependencies: FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_HYB_EXT.1.1 The TOE shall only use [**selection**: *fingerprint, iris, face, voice, vein*], [**assignment**: *other modality*] as the biometric component of the hybrid authentication mechanism.

Application Note 34

A hybrid authentication mechanism is one where a user has to submit a combination of biometric sample and PIN or password with both to pass and without the user being made aware of which factor failed, if either fails. If this mechanism is selected in the [MDFPP], the above component shall also be selected.

12.2. Protection of the TSF (FPT)

12.2.1. Biometric data processing (FPT_BDP_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to protect plaintext biometric data using security functions provided by the TOE environment.

Component levelling

Figure 6. Component levelling

FPT_BDP_EXT.1 Biometric data processing requires the TSF to process plaintext biometric data within the security boundary of the secure execution environment.

FPT_BDP_EXT.2 No Biometric data transmission requires the TSF not to transmit plaintext biometric data outside the security boundary of the secure execution environment.

FPT_BDP_EXT.3 Biometric data storage requires the TSF not to store plaintext biometric data outside the security boundary of the secure execution environment.

Management: FPT_BDP_EXT.1, FPT_BDP_EXT.2, FPT_BDP_EXT.3

There are no management activities foreseen.

Audit: FPT_BDP_EXT.1, FPT_BDP_EXT.2, FPT_BDP_EXT.3

There are no auditable events foreseen.

FPT_BDP_EXT.1 Biometric data processing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_BDP_EXT.1.1 The TSF shall process any plaintext biometric data used to generate templates and perform sample matching within the security boundary of the secure execution environment.

Application Note 35

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

FPT_BDP_EXT.2 No Biometric data transmission

Hierarchical to: No other components Dependencies: No dependencies

FPT_BDP_EXT.2.1 The TSF shall not transmit any plaintext biometric data outside the security boundary of the secure execution environment.

Application Note 36

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

FPT_BDP_EXT.3 Biometric data storage

Hierarchical to: No other components

Dependencies: No dependencies

FPT_BDP_EXT.3.1 The TSF shall not store any plaintext biometric data outside the security boundary of the secure execution environment.

Application Note 37

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

12.2.2. Protection of biometric template (FPT_PBT_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to protect templates.

Component levelling

Figure 7. Component levelling

FPT_PBT_EXT.1 Protection of biometric template requires the TSF to protect templates.

Management: FPT_PBT_EXT.1

There are no management activities foreseen.

Audit: FPT_PBT_EXT.1

There are no auditable events foreseen.

FPT_PBT_EXT.1 Protection of biometric template

Hierarchical to: No other components

Dependencies: No dependencies

FPT_PBT_EXT.1.1 The TSF shall protect the template [**selection**: *using a PIN as an additional factor, using a password as an additional factor*], [**assignment**: *other circumstances*]].

Application Note 38

Annex A Consistency Rationale between this PP-Module and MDFPP explains how the TOE in cooperation with its environment shall protect biometric data in detail.

13. Annex A Consistency Rationale between this PP-Module and MDFPP

13.1. Overview

This Annex describes consistency rationale between this PP-Module and [MDFPP].

The TOE in this PP-Module is comprised of biometric capture sensors and firmware/software that provide functions described in Section [TOE design]. The TOE is invoked by the mobile device (i.e. TOE environment) when user's biometric characteristics is presented to the sensor. The TOE 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 [MDFPP] so that the TOE can work as specified in this PP-Module. The next section explains which SFRs in the [MDFPP] are directly relevant to the TOE security functionality.

13.2. Relevant SFRs in the MDFPP

Relation between SFRs defined in this PP-Module and in the [MDFPP] is described below. **Bold SFRs** are those defined in this PP-Module and *italicized SFRs* are those defined in [MDFPP].

13.2.1. Password authentication

Mobile device shall implement the Password Authentication Factor as required by the *FIA_UAU.5.1*. This password authentication is used as an alternative authentication mechanism when the user is rejected by the mobile biometric verification.

This PP-Module assumes that above requirements are satisfied by the mobile device as defined in OE.Alternative.

13.2.2. Invocation of the TOE

For any modality selected in *FIA_UAU.5.1*, mobile device shall invoke the TOE to unlock the device under the condition specified in *FIA_UAU.6.1(2)*. Mobile device shall also authenticate the user following the rule specified in *FIA_UAU.5.2*.

This PP-Module assumes that above requirements are satisfied by the mobile device as defined in OE.Authentication.

The TOE shall implement a mobile biometric verification mechanism that satisfies SFRs defined in this PP-Module. This means that same modality shall be selected in **FIA_MBV_EXT.1.1**, and relevant criteria and its error rate shall be specified in **FIA_MBV_EXT.1.2**. If multiple modalities are selected in *FIA_UAU.5.1*, **FIA_MBV_EXT.1** shall be iterated for each modality. If hybrid is selected in *FIA_UAU.5.1*, **FIA_HYB_EXT.1** shall also be selected. The TOE shall also enrol all modalities selected as specified in **FIA_MBE.EXT.1**, assure the quality of samples and templates as specified in **FIA_MBV.EXT.2** and **FIA_MBE.EXT.2** and prevent use of artificial presentation attack instruments

during the mobile biometric verification as specified in **FIA_MBV.EXT.3**. The TOE may also prevent use of artificial presentation attack instruments during the mobile biometric enrolment as specified in **FIA_MBV.EXT.3**.

All SFRs in bold are defined in Security Functional Requirements, Selection-Based Requirements and Optional Requirements in this PP-Module.

13.2.3. Handling the verification outcome

Mobile device shall take appropriate actions after receiving the verification outcome from the TOE as defined in *FIA_AFL_EXT.1*.

FIA_AFL_EXT.1 defines rules regarding how the authentication factors interact in terms of unsuccessful authentication and actions mobile device shall take when number of unsuccessful authentication attempts surpass the pre-defined number. Mobile device also shall apply authentication throttling after failed biometric verification, as required by *FIA_TRT_EXT.1.1*.

This PP-Module assumes that above requirements are satisfied by the mobile device as defined in OE.Authentication.

13.2.4. Protection of the TOE and its biometric data

Mobile device shall provide the secure execution environment (e.g. restricted operational environment) so that TOE can work securely. This secure execution environment guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. This secure execution environment is out of scope of the TOE and shall be provided by the mobile device and evaluated based on [MDFPP]. However, ST author shall explain how such secure execution environment is provided by the mobile device for the TOE, as required by [SD]. Mobile device shall also keep secret any sensitive information regarding the biometric when mobile device receives the verification outcome from the TOE, as required by *FIA_UAU.7.1*, and provide cryptographic support to encrypt or decrypt biometric data as required by *FCS class*.

This PP-Module assumes that above requirements are satisfied by the mobile device as defined in OE.Protection.

However, the TOE shall use this secure execution environment correctly to protect biometric data and satisfy the following requirements:

- The TOE shall process any plaintext biometric data (e.g. capturing biometric characteristic, creating samples, features and templates) for mobile biometric enrolment and verification within the boundary of the secure execution environment. This implies that:
  - Any part of the TOE that processes plaintext biometric data shall be within the boundary of the secure execution environment. For example, the biometric capture sensor shall be configured to be within the boundary of the secure execution environment, so that only the secure execution environment can access to the sensor and the data captured. Any software modules that process plaintext biometric data shall run within the boundary of the secure execution environment.
  - Plaintext biometric data shall never be accessible from outside the secure execution environment, and any entities outside the secure execution environment can only access the

result of process of biometric data (e.g. success or failure of mobile biometric verification) through the interface provided by the TOE.

- The TOE shall not transmit any plaintext biometric data outside of the secure execution environment.

If the TOE stores the part of biometric data outside the secure execution environment, the TOE shall protect such data so that any entities running outside the secure execution environment can't get access to any plaintext biometric data. ST author shall explain what biometric data resides outside the secure execution environment as required by [SD] and if no data resides outside the environment, requirements below is implicitly satisfied.

- The TOE shall not store any plaintext biometric data outside the secure execution environment. As described in Section [TOE design], the TOE can store templates in the enrolment database. The TOE shall encrypt templates using cryptographic service provided by the mobile device within the secure execution environment before storing them in the database, even if the mobile device storage itself is encrypted by the mobile device.
- The TOE may override encrypted biometric data in the storage when no longer needed. For example, the TOE may override encrypted template when it is revoked. This is an optional requirement.

The TOE shall also protect templates so that only the user of the mobile device can access them. This means that the TOE shall only allow authenticated user by the Password Authentication Factor to access (e.g. add or revoke) the template.

- The TOE shall control access to, including adding or revoking, the templates.

The above requirements are defined as **FPT_PBT_EXT.1**, **FPT_BDP_EXT.1**, **FPT_BDP_EXT.2** and **FPT_PBT_EXT.3** in Security Functional Requirements and **FDP_RIP.2** in Optional Requirements in this PP-Module.

13.2.5. Management of the TOE configuration

Mobile device shall enable/disable the BAF as required by *FMT_SMF_EXT.1 (Management function 23)*, and revoke the BAF as *FMT_SMF_EXT.1 (Management Function 46)*. Any change to the BAF (e.g. adding or revoking templates) requires re-authentication via the Password Authentication Factor as required by *FIA_UAU.6.1(1)*.

This PP-Module assumes that above requirements are satisfied by the TOE environment as defined in OE.Protection.