collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -

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 biometric enrolment and verification on the computer. 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.
- [MDFPP] Protection Profile for Mobile Device Fundamentals, Version:3.3.
- [PPC-MDF] PP-Configuration for Protection Profile for Mobile Device Fundamentals and collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -, December 20, 2019, Version 0.92.
- [SD] Evaluation Activities for collaborative Protection Profile Module for Biometric enrolment and verification - for unlocking the device -, December 20, 2019, Version 0.92.
- [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
- [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 and ISO/IEC 30107-1. 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 biometric enrolment and verification.

Artefact

Biometric characteristic or object used in a presentation attack (e.g. artificial or abnormal biometric characteristics). Accompanying [SD] specifies artefacts that the evaluator should consider for the CC evaluation. Artefacts here are specifically artificially generated Presentation Attack Instruments (PAI), not natural ones.

Attempt

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

Biometric Authentication Factor (BAF)

Authentication factor used for 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.

Computer

A self-contained device which is composed of a hardware platform and its system software (operating system and applications). The device is typically some sort of general purpose computing platform, such as a laptop, tablet or smartphone that is designed to be portable (though this is not required).

Computer User (User)

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

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 Computer, with most functionalities unavailable for use. User authentication is required to access full functionality.

(Biometric) Modality

A type or class of biometric system, such as fingerprint recognition, facial recognition, eye/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.

(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 Computer 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.

(Biometric) Species

The biometric species is the type of Presentation Attack Instrument (PAI) that has been created such as a photo, mold or mask (as appropriate for the modality being tested).

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
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

Version	Date	Description
0.9	5th August, 2019	Updates based on Public Review Draft 1 comments
0.9	5th December, 2019	Updates to make PAD optional
0.92	December 20, 2019	Public Review Draft 2

3. PP-Module Introduction

3.1. PP-Module Reference

- PP-Module Reference: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -
- PP-Module Version: 0.92
- PP-Module Date: 2019-12-20

3.2. Base PP identification

Base PP of this PP-Module is identified in the appropriate PP-Configuration.

3.3. TOE Overview

3.3.1. TOE main security features

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

a) 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 computer 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 computer's User Interface).

b) 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 computer. 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 computer.

Examples of biometric characteristic used by the TOE are: fingerprint, face, eye, 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.

3.3.2. TOE Design

The TOE is fully integrated into the computer 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 biometric enrolment and verification processes rely on.

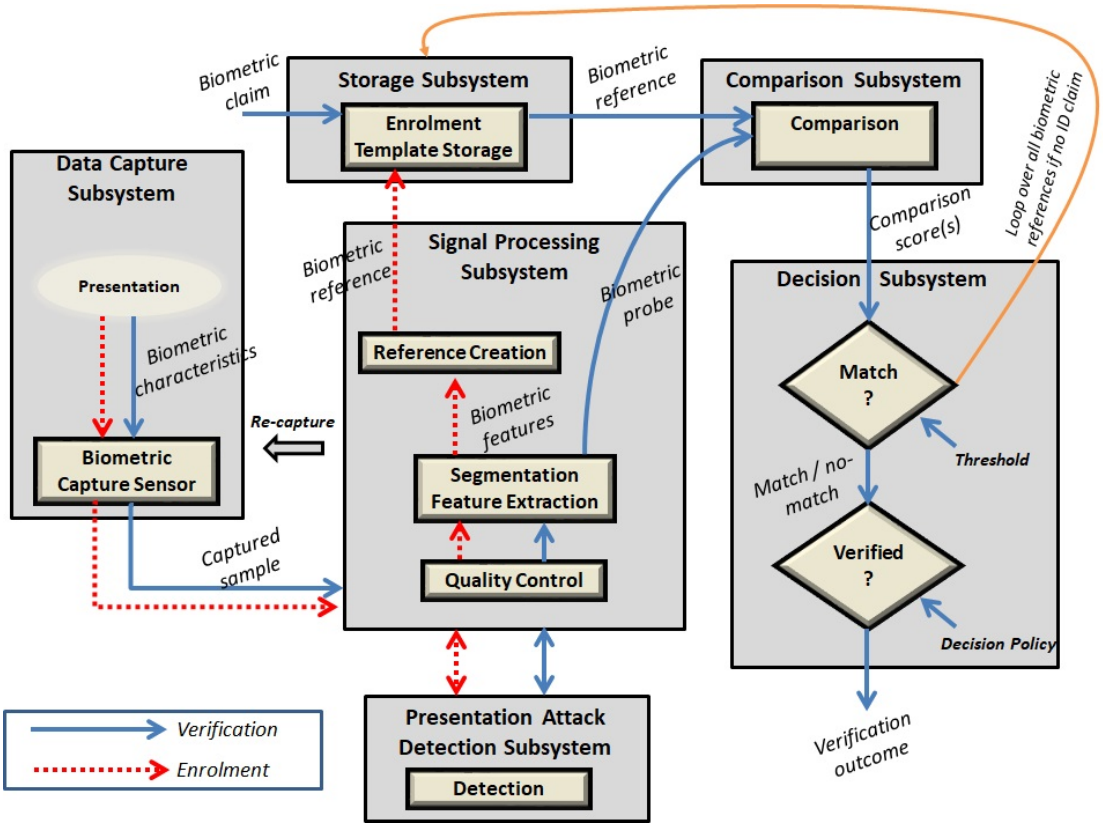

Figure 1. Generic representation of a TOE

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 computer (Data Storage Subsystem)

- Comparing captured features with data contained in one or more templates (Comparison Subsystem)
- Optionally detecting the presentation attacks using an artefact
- Deciding how well features and any template match, and indicating whether or not a verification of the user has been achieved (Decision Subsystem)

3.3.3. Relation between TOE and Computer

The TOE is reliant on the computer itself to provide overall security of the system. This PP-Module is intended to be used with a base PP, and the base PP 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 as part of the base PP evaluation.

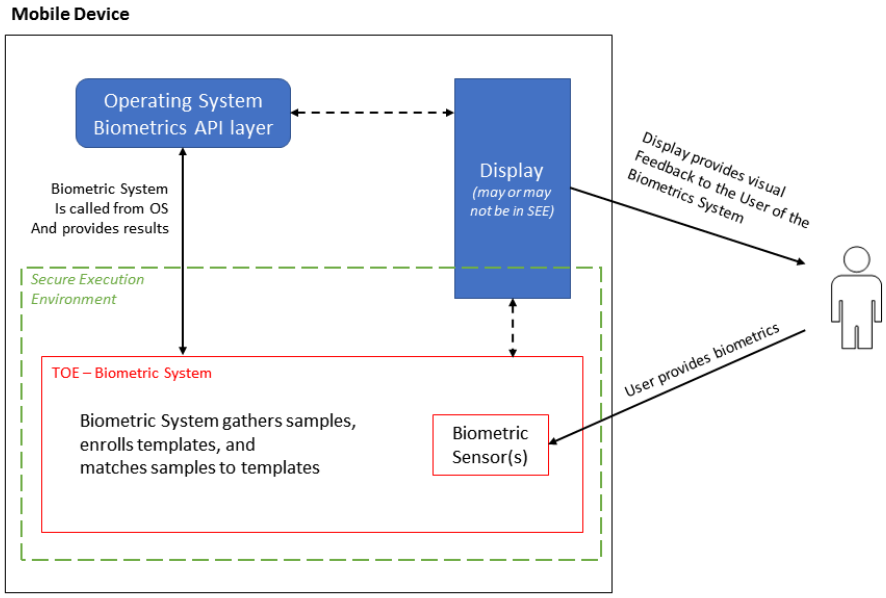

Figure 2. Generic relations between the TOE and the computer environment

3.3.4. TOE Use Case

The computer 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 biometric verification. The following use cases describe how and why 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.

3.3.4.1. USE CASE 1: Biometric verification for unlocking the computer

For enhanced security that is easy to use, the computer may implement 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 their own biometric characteristic to unlock access to the computer. In this use case, the computer is not supposed to be used for security sensitive services through the biometric verification.

The main concern of this use case is the accuracy of the biometric verification (i.e. FAR/FMR and FRR/FNMR). Security assurance for computer that the TOE relies on should be handled by the base PP.

This use case assumes that the computer is configured correctly to enable the biometric verification by the biometric system administrator. The user of the computer 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. Presentation attacks during biometric enrolment and verification may be out of scope, but optionally addressed. FTE is not a security relevant criterion for this use case.

3.3.4.2. USE CASE 2: 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 or PP-Module should be developed at higher assurance level for this use case.

Computers 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 presentation attack detection.

4. Consistency rationale

Consistency between the base PP and this PP-Module is demonstrated in the appropriate PP-Configuration.

5. Conformance Claims

5.1. Conformance statement

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,
- all assurance requirements are inherited from the base PP,
- does not claim conformance to any other security functional packages.

5.2. Conformance type

In order to be conformant to this PP-Module, a ST shall demonstrate Exact Conformance. Exact Conformance requires the ST to contain all of the SFRs in Security Functional Requirements (these are the mandatory SFRs). The ST may includes 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.

5.3. Evaluation activities

This PP-Module requires the use of evaluation activities defined in [SD].

6. 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: Biometric verification for unlocking the computer.

Note that as a PP-Module, all threats, assumptions, and OSPs defined in the base PP 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 base PP in more comprehensive detail due to the specific capabilities provided by a biometric system.

6.1. 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).

6.2. Organizational Security Policies

OSP.Enrol

The TOE shall enrol a user for 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 biometric verification.

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 biometric verification.

6.3. Assumptions

A.Alternative

It is assumed that the TOE environment provides an alternative authentication mechanism as a complement to 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 biometric verification (False Rejection).

A.Authentication

It is assumed that the TOE environment invokes the TOE for 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.

7. Security Objectives

This PP-Module defines the following security objectives.

7.1. Security Objectives for the TOE

O.BIO_Verification

The TOE shall provide a 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 biometric verification.

SFR Rationale:

Requirements to provide a 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 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 biometric verification.

SFR Rationale:

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

Application Note 2

A user shall be authenticated using a Password Authentication Factor to enrol his/herself.

Application Note 3

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.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 4

The TOE and TOE environment (i.e. the computer) shall satisfy relevant requirements defined in this PP-Module and base PP respectively to protect biometric data.

7.2. Security Objectives for the Operational Environment

OE.Alternative

The TOE environment shall provide an alternative authentication mechanism as a complement to 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 biometric verification (False Rejection).

Application Note 5

The TOE environment (i.e. the computer) shall satisfy relevant requirements defined in base PP.

Application Note 6

The TOE environment (i.e. the computer) shall provide an alternative authentication mechanism such as a Password Authentication Factor.

OE.Authentication

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

Application Note 7

Appropriate actions taken by the computer are unlocking the computer 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 8

The TOE and TOE environment (i.e. the computer) shall satisfy relevant requirements defined in this PP-Module and base PP respectively to protect biometric data.

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 9

Computer shall be configured by the user as required by base PP.

7.3. 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 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 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 biometric verification and create sufficient quality of templates.
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.

8. Security Functional Requirements

8.1. 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 within square brackets**] indicates the type of operation.

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

8.2. Identification and Authentication (FIA)

8.2.1. FIA_MBE_EXT.1 Biometric enrolment

FIA_MBE_EXT.1.1

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

Application Note 10

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

8.2.2. FIA_MBE_EXT.2 Quality of biometric templates for biometric enrolment

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

Application Note 11

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

8.2.3. FIA_MBV_EXT.1 Biometric verification

FIA_MBV_EXT.1.1

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

Application Note 12

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

Application Note 13

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

Application Note 14

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 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.

8.2.4. FIA_MBV_EXT.2 Quality of biometric samples for biometric verification

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

Application Note 15

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

8.3. Protection of the TSF (FPT)

8.3.1. 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 16

The Consistency Rationale in the appropriate PP-Configuration explains how the TOE in cooperation with its environment shall protect biometric data in detail.

8.3.2. 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 17

The Consistency Rationale in the appropriate PP-Configuration explains how the TOE in cooperation with its environment shall protect biometric data in detail.

8.3.3. 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 18

The Consistency Rationale in the appropriate PP-Configuration explains how the TOE in cooperation with its environment shall protect biometric data in detail.

8.3.4. 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 19

The Consistency Rationale in the appropriate PP-Configuration explains how the TOE in cooperation with its environment shall protect biometric data in detail.

9. Security Assurance Requirements

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.

10. Selection-Based Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that shall 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.

The PP-Module does not contain any selection-based requirements.

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 biometric enrolment

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

11.1.2. FIA_MBV_EXT.3 Presentation attack detection for biometric verification

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

Application Note 20

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

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 21

The Consistency Rationale in the appropriate PP-Configuration explains how the TOE in cooperation with its environment shall 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 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. Biometric enrolment (FIA_MBE_EXT)

12.1.1.1. 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.

12.1.1.2. Component levelling

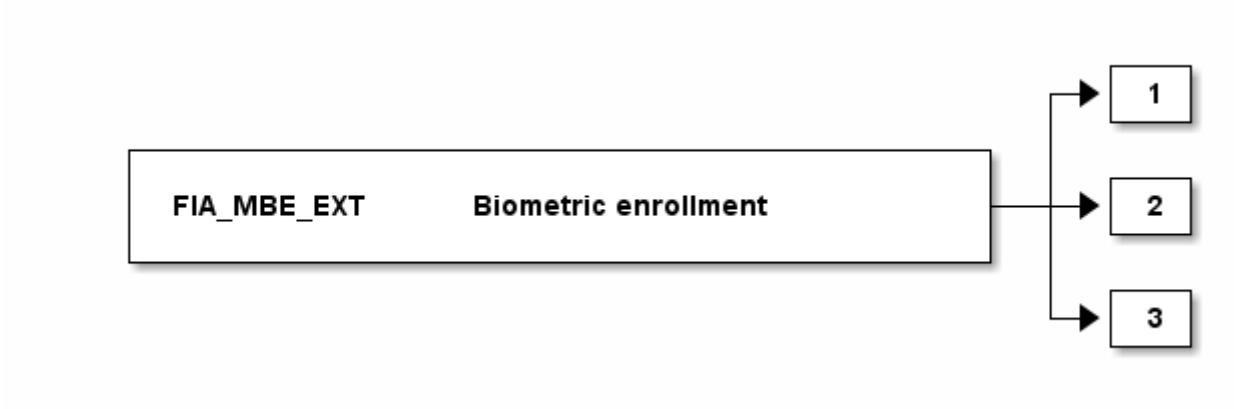

Figure 3. Component levelling

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

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

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

12.1.1.3. Management: FIA_MBE_EXT.1

There are no management activities foreseen.

12.1.1.4. 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.

12.1.1.5. 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.

12.1.1.6. 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 biometric enrollment

12.1.1.7. 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

12.1.1.8. 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.

12.1.1.9. FIA_MBE_EXT.2 Quality of biometric templates for biometric enrolment

Hierarchical to: No other components

Dependencies: FIA_MBE_EXT.1 Biometric enrolment

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

12.1.1.10. FIA_MBE_EXT.3 Presentation attack detection for biometric enrolment

Hierarchical to: No other components

Dependencies: FIA_MBE_EXT.1 Biometric enrolment

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

12.1.2. Biometric verification (FIA_MBV_EXT)

12.1.2.1. 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.

12.1.2.2. Component levelling

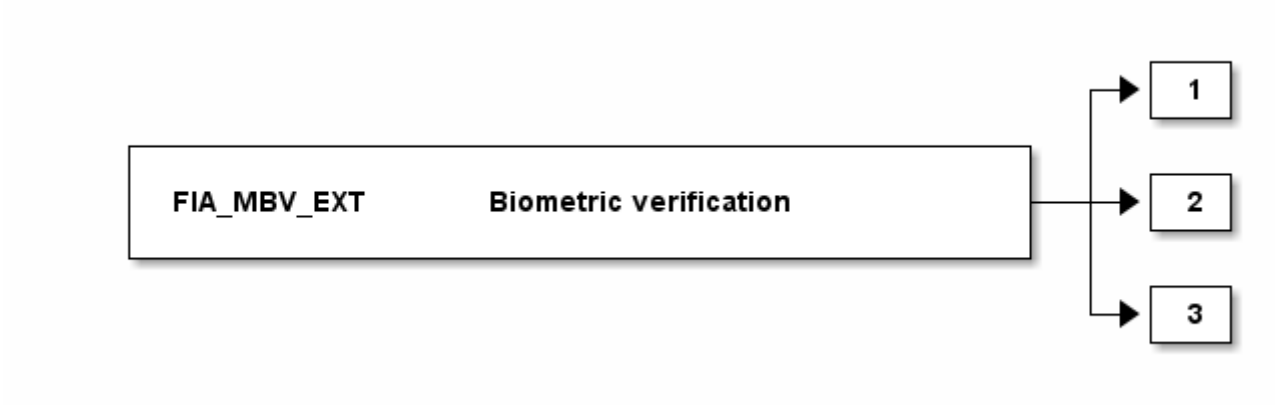

Figure 4. Component levelling

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

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

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

12.1.2.3. 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.

12.1.2.4. 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.

12.1.2.5. 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.

12.1.2.6. 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 biometric verification

12.1.2.7. 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

12.1.2.8. 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 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*].

12.1.2.9. FIA_MBV_EXT.2 Quality of biometric samples for biometric verification

Hierarchical to: No other components.

Dependencies:

FIA_MBE_EXT.1 Biometric enrolment

FIA_MBV_EXT.1 Biometric verification

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

12.1.2.10. FIA_MBV_EXT.3 Presentation attack detection for biometric verification

Hierarchical to: No other components

Dependencies:

FIA_MBE_EXT.1 Biometric enrolment

FIA_MBV_EXT.1 Biometric verification

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

12.2. Protection of the TSF (FPT)

12.2.1. Biometric data processing (FPT_BDP_EXT)

12.2.1.1. 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.

12.2.1.2. Component levelling

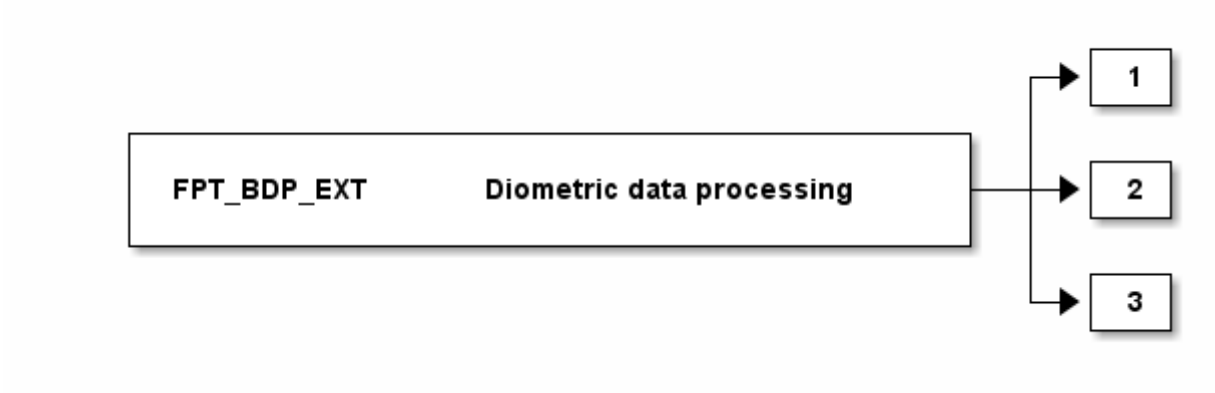

Figure 5. Component levelling

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.

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

There are no management activities foreseen.

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

There are no auditable events foreseen.

12.2.1.5. 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.

12.2.1.6. 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.

12.2.1.7. 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.

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.

12.2.2.1. Component levelling

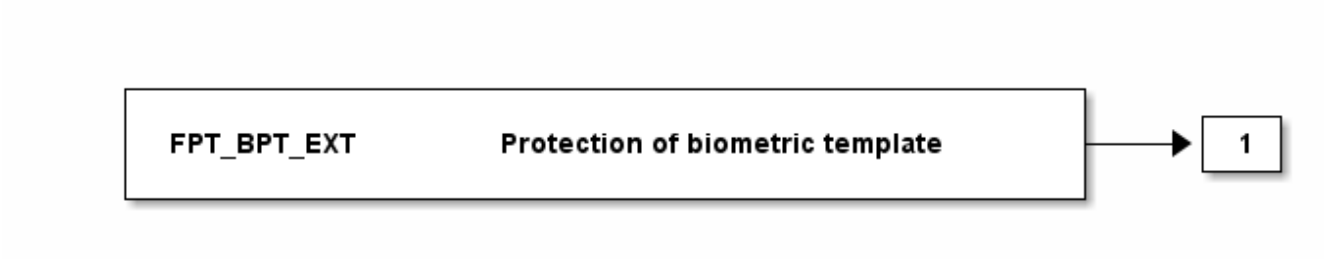

Figure 6. Component levelling

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.

12.2.2.2. 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*]].