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

Version 1.1, TBD, 2021

Table of Contents

Acknowledgements

This collaborative Protection Profile module (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.

Chapter 1. Preface

1.1. 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 [BIOSD].

1.2. 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.

1.3. Intended Readership

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

Although the PP-Module and Supporting Document [BIOSD] 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.

1.4. 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.
- [PP_OS] Protection Profile for General Purpose Operating Systems.
- [PP_MD_V3.3] 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 -, TBD, 2021, Version 1.0 [CFG-MDF-BIO].

- [BIOSD] Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -, TBD, 2021, Version 1.1 - [BIOSD].
- [ISO/IEC 19795-1] Biometric performance testing and reporting — Part 1: Principles and framework, First edition.
- [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.
- [NIST800-63B] NIST Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management, June 2017

1.5. Glossary

For the purpose of this PP-Module, the following terms and definitions are 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 [BIOSD] specifies artefacts that the evaluator should consider for the CC evaluation. Specifically, the artefacts here are 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.

(Non-Biometric) Authentication Factor (NBAF)

Evidence to assert the identity of an individual based on knowledge or possession (e.g. password, PIN, smartcard).

Biometric Authentication Factor (BAF)

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

Biometric Characteristic

Biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition.

Biometric Claim

A claim that a user presenting a biometric sample is or is not the source of a specified or unspecified biometric 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, authentication factor (unless tied to the biometric modality), demographic information, and authorizations.

Biometric Enrolment

The initial process of collecting biometric data samples from a person and subsequently storing the data in a reference template representing a user's identity to be used for later comparison.

Biometric Probe

Biometric sample or biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric template(s).

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). *In this version, the term Computer is used as a synonym for Mobile device. However, in the future version, this PP-Module will be updated to allow to use with the latest version of [PP_OS] and this italic text will also be removed.*

Computer User (User)

The individual authorized to physically control and operate the Computer, usually the device owner. This person is responsible for configuring the TOE.

Developer Defined Quality Assessment Method

Assessment criteria defined by the developer used to measure the quality of a Biometric Sample captured by the system.

Failure-To-Enrol 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 biometric 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 biometric characteristic from the same user supplying the sample.

False Reject Rate (FRR)

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

(Biometric) 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.

Imposter Attack Presentation Accept Rate (IAPAR)

In a full-system evaluation of a verification system, proportion of impostor presentation attacks using the same artefact type that result in a accept.

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, vein, voice recognition, signature/sign, and others.

Presentation

Submission of a single biometric sample on the part of a user.

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.

Separate Execution Environment (SEE)

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.

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 one's biometric characteristics as if attempting successful verification against one's own template, but the comparison is made against the template of another user.

1.6. Revision History

Table 1. Revision history

Version	Date	Description
0.1	October 24, 2017	Preliminary draft for the Berlin iTC session
0.2	February 26, 2018	First version uploaded to the repo in the Github for review
0.3	March 9, 2018	Add SFRs and make editorial changes
0.6	July 13, 2018	Add ECDs and make editorial changes
0.8	May 1, 2019	Convert the cPP as of 11th Jan, 2019 into the PP-Module
0.9	August 5, 2019	Updates based on Public Review Draft 1 comments
0.9	December 5, 2019	Updates to make PAD optional
0.92	December 20, 2019	Public Review Draft 2
0.95	March 13, 2020	Proposed Release
1.0	May 11, 2020	Public Release
1.1	TBD, 2021	Incorporated TDs and NIAP comments for PP_MD_V3.3 integration

Chapter 2. PP-Module Introduction

2.1. PP-Module Reference

- PP-Module Reference: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module]
- PP-Module Version: 1.1
- PP-Module Date: TBD, 2021

2.2. Base-PP identification

This PP-Module is intended for use with the following Base-PP: Protection Profile for Mobile Device Fundamentals [PP_MD_V3.3].

This Base-PP is valid because biometric enrolment and verification may be a specific type of stand-alone software application or a built-in component of a computer. The biometric enrolment and verification functionality defined by this PP-Module will rely on the Base-PP. The biometric enrolment and verification functionality defined by this PP-Module will rely on the Base-PP and Section PP_MD_V3.3 Security Functional Requirements Direction of this PP-Module describes the relevant functionality for the Base-PP, including specific selections, assignments, or inclusion of optional requirements that must be made as needed to support the biometric enrolment and verification functionality.

2.3. TOE Overview

2.3.1. TOE main security features

This is a collaborative Protection Profile Module (PP-Module) used to extend a Base-PP for a computer that implements 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. The biometric enrolment and verification processes are described in the following sections.

2.3.1.1. 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 NBAF can enrol or revoke one's own templates. Multiple templates may be enroled, as separate entries uniquely identified by the TOE, and optionally uniquely identifiable by the user (through the computer's User Interface).

2.3.1.2. Biometric Verification

During the verification process, a user presents one's 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 enroled 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 [BIOSD] defines the Evaluation Activities.

2.3.2. 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.

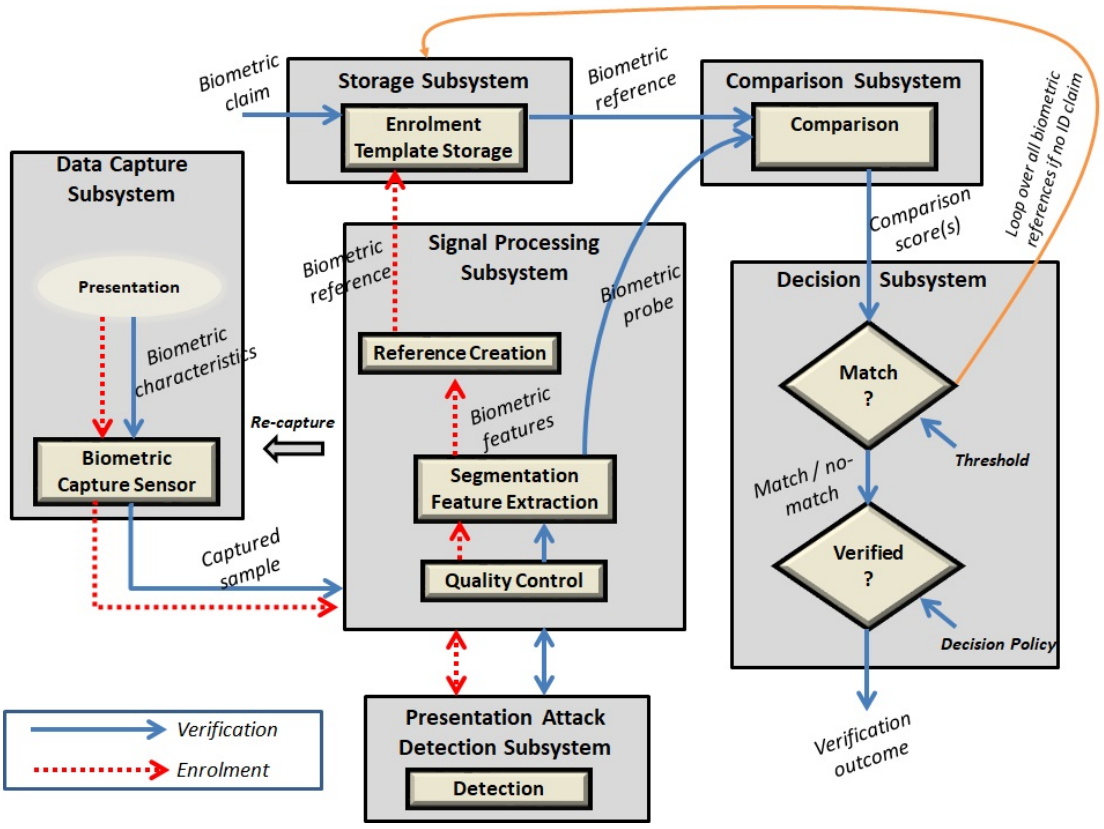

Figure 1. Generic representation of a TOE

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

2.3.3. 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 NBAF 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 Separate Execution Environment that guarantees the TOE and its data to be protected with respect to confidentiality and integrity

The specification of the above security functions is out of scope of this PP-Module and are part of the Base-PP.

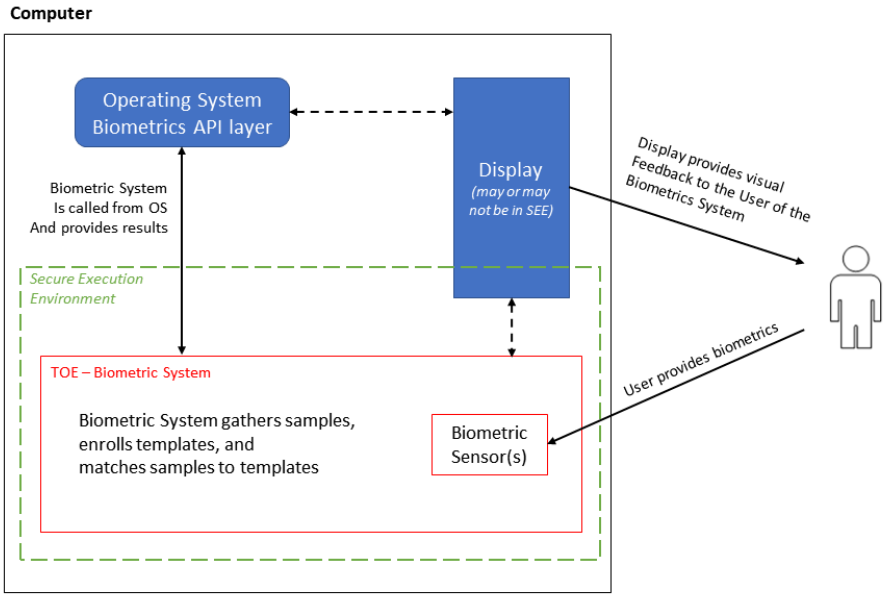

Figure 2. Generic relation between the TOE and the computer environment

2.3.4. 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.

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

This use case is applicable for any computers such as a desktop, laptop, tablet or smartphone that implement biometric enrolment and verification functionality. For enhanced security that is easy to use, the computer may implement biometric verification on a computer once it has been "unlocked". The initial unlock is generally done by a NBAF which is required at startup (or possibly after some period of time), and after that, the user is able to use one's 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 user, who acts as the biometric system administrator in this use case.

It is also assumed that the user enrols to the biometric system 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.

2.3.4.2. USE CASE 2: Biometric verification for security sensitive service

This use case is an example of another use case that is not 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 the NBAF 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.

Chapter 3. Conformance Claims

3.1. Conformance statement

As defined by the references [CC1], [CC2] and [CC3], when the Base-PP is the PP_MD_V3.3, this PP-Module:

- conforms to the requirements of Common Criteria v3.1, Revision 5,
- is Part 2 extended,
- is Part 3 extended,
- all assurance requirements are inherited from the Base-PP,
- does not claim conformance to any other security functional packages or Protection Profiles.

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- PP-Module for Virtual Private Network (VPN) Clients, Version 2.2
- PP-Module for MDM Agents, Version 1.0

3.2. Evaluation activities

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

Chapter 4. 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.

4.1. Threats

T.Casual_Attack

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

4.2. 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.

4.3. Assumptions

This PP-Module does not define any assumptions.

Chapter 5. Security Objectives

This PP-Module defines the following security objectives.

5.1. 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 are 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. Corresponding error rates are specified in 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 templates of sufficient quality in order to meet the relevant error rates for biometric verification.

SFR Rationale:

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

Application Note 2

A user enroling to the biometric system will have been authenticated using a NBAF, as specified in FIA_MBE_EXT.1.1.

Application Note 3

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

O.Protection

The TOE shall protect biometric data using the Separate Execution Environment provided by the TOE environment during runtime and storage.

SFR Rationale:

Requirements to control access to the template defined in FPT_PBT_EXT.1. FPT_BDP_EXT.1,

FPT_KST_EXT.1 (refined from [PP_MD_V3.3]) and FPT_KST_EXT.2 (refined from [PP_MD_V3.3]) require the TOE to protect the biometric data with support from the TOE environment. Optional requirements to protect the residual biometric data are defined as FDP_RIP.2 in Optional Requirements.

Application Note 4

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

5.2. Security Objectives for the Operational Environment

OE.Protection

The TOE environment shall provide a Separate Execution Environment to protect the TOE, the TOE configuration and biometric data during runtime and storage.

Application Note 5

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

5.3. 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 Definition 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 to disallow an unenroled user from impersonating 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.

Chapter 6. Security Functional Requirements

6.1. 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.

6.2. PP_MD_V3.3 Security Functional Requirements Direction

In a PP-Configuration that includes the [PP_MD_V3.3], the biometric enrolment and verification is expected to rely on some of the security functions implemented by the computer as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by TOE Security Functional Requirements.

Full evaluation activities are not repeated in the [BIOSD] for the requirements in this section that are references to the [PP_MD_V3.3]; only the additional testing needed to supplement what has already been captured in the [PP_MD_V3.3] is included in the [BIOSD]

6.2.1. Modified SFRs

The SFRs listed in this section are defined in the [PP_MD_V3.3] and relevant to the secure operation of the biometric enrolment and verification. It is necessary for the ST author to complete selections and/or assignments for these SFRs in a specific manner in order to ensure that the functionality provided by the mobile device is consistent with the functionality required by the biometric enrolment and verification in order for it to conform to this PP-Module.

6.2.1.1. Class: Cryptographic Support (FCS)

This PP-Module does not modify SFRs in FCS class as it is defined in the [PP_MD_V3.3]. However, note that BAF must be illustrated in the key hierarchy diagram and all keys created upon successful biometric enrolment and verification must be generated, derived, combined, released and destroyed according to SFRs in this class.

6.2.1.2. FCS_CKM_EXT.4 Key Destruction

This SFR is identical to what is defined in the [PP_MD_V3.3]. The change is to the application note.

Application Note: For the purposes of this requirement, plaintext keying material refers to

authentication data, passwords, secret/private symmetric keys, private asymmetric keys, data used to derive keys, values derived from passwords, etc. **Biometric data used for enrolment or verification are considered critical security parameters that must be destroyed when no longer needed.**

Application Note 6

The Application Note following FCS_CKM_EXT.4.2 is modified to add the text to include biometric data as a critical security parameter to ensure it is handled properly by the TSF.

6.2.1.3. FPT_AEX_EXT.4 Domain Isolation

This SFR is identical to what is defined in the [PP_MD_V3.3]. The change is to the application note.

Application Note: In addition to the TSF software (e.g., kernel image, device drivers, trusted applications) that resides in storage, the execution context (e.g., address space, processor registers, per-process environment variables) of the software operating in a privileged mode of the processor (e.g., kernel, **other processor modes**) **or on separate processors**, as well as the context of the trusted applications is to be protected. In addition to the software, any configuration information that controls or influences the behavior of the TSF is also to be protected from modification by untrusted subjects.

Application Note 7

This application note explicitly adds more support for additional processor modes (e.g. the Secure/Normal World modes defined in a Trusted Execution Environment) or separate processors (e.g. a secure element) that may be present and used for the processing of biometric data. Biometric components should be considered as TSF software being protected by these mechanisms, defined as the separate execution environment.

6.2.1.4. FPT_KST_EXT.1 Key Storage

FPT_KST_EXT.1.1

The TSF shall not store any plaintext key material **or biometric data** in readable non-volatile memory.

Application Note 8

This SFR is functionally identical to what is defined in the [PP_MD_V3.3] with the addition of biometric data as key materials to be protected. Plaintext biometric data to be protected includes any data used to generate templates or perform sample comparisons from the initial data capture, as well as the comparison score.

6.2.1.5. FPT_KST_EXT.2 No Key Transmission

FPT_KST_EXT.2.1

The TSF shall not transmit any plaintext key material **or biometric data** outside the security boundary of the TOE.

Application Note 9

This SFR is functionally identical to what is defined in the [PP_MD_V3.3] with the addition of biometric data as plaintext key materials that must not be transmitted off-device.

6.2.2. Additional SFRs

There are no additional SFRs that must be claimed only in cases where the [PP_MD_V3.3] is the claimed Base-PP.

6.3. TOE Security Functional Requirements

This section lists SFRs for the biometric enrolment and verification.

6.3.1. Identification and Authentication (FIA)

6.3.1.1. 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

A user enroling to the biometric system will have been authenticated using a NBAF, as specified in FIA_MBE_EXT.1.1.

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

FIA_MBE_EXT.2.1

The TSF shall only use biometric samples of sufficient quality for enrolment. Sufficiency of sample data shall be determined by measuring sample with [**selection**: [[**assignment**: *quality metric standard*] using a threshold of [**assignment**: *quality metric threshold*]], [**assignment**: *developer defined quality assessment method*]].

6.3.1.3. FIA_MBV_EXT.1 Biometric verification

FIA_MBV_EXT.1.1

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

FIA_MBV_EXT.1.2

The TSF shall provide a biometric verification mechanism with the [**selection**: *FMR, FAR*] not exceeding [**assignment**: *value equal to or less than 0.01% (1:10^4)*] for the upper bound of [**assignment**: *value equal to or greater than 80%*] confidence interval and, [**selection**: *FNMR, FRR*] not exceeding [**assignment**: *value equal to or less than 5% (5:100)*] for the upper bound of [**assignment**: *value equal to or greater than 80%*] confidence interval.

Application Note 11

Consider the following factors when setting values of FMR, FAR, FNMR and FRR.

a. Allowed maximum values defined in the standards

   For example, [NIST800-63B] requires that FMR 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 that fingerprint verification have the FAR lower than 0.002% and recommended to have the FRR lower than 10%. While the PP-Module does not provide any recommendation for those error rates other than minimum error rates, the ST author should set appropriate error rates referring those values.

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.

ISO/IEC 19795-1 recommends following “rule of 3” (i.e. 95% confidence interval) if there is no error observed during the performance testing. The ST author should assign appropriate confidence interval referring such relevant standards.

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, the 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 [BIOSD]. Normally the target error rates will directly influence the size of the test subjects, the time and cost of the testing. [BIOSD] describes how those error rates should be evaluated in an objective manner.

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

FIA_MBV_EXT.2.1

The TSF shall only use biometric samples of sufficient quality for verification. Sufficiency of sample data shall be determined by measuring sample with [**selection**: [[**assignment**: *quality metric standard*] using a threshold of [**assignment**: *quality metric threshold*]], [**assignment**: *developer defined quality assessment method*]].

6.3.2. Protection of the TSF (FPT)

6.3.2.1. FPT_BDP_EXT.1 Biometric data processing

FPT_BDP_EXT.1.1

Processing of plaintext biometric data shall be inside the separate execution environment in runtime.

Application Note 12

All TSF code and plain biometric data must be executed and retained inside the separate execution environment.

FPT_BDP_EXT.1.2

Transmission of plaintext biometric data between the capture sensor and the separate execution environment shall be isolated from the main computer operating system on the TSF in runtime.

Application Note 13

This is specifically about the transmission of biometric data within the device between components, and not to external systems (such as an export of biometric data).

6.3.2.2. 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*]].

6.4. TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 3. Mapping between SFRs and Security Objectives

Objective	Addressed By	Rationale
O.BIO_Verification	FIA_MBV_EXT.1	This SFR supports the objective by defining the minimum accuracy of the biometric authentication methods that the TSF must support for verification.
	FIA_MBV_EXT.2	This SFR supports the objective by requiring the TSF to enforce a minimum quality standard on the biometric data used for verification.
	FIA_MBV_EXT.3 (optional)	This SFR supports the objective by requiring the TSF to detect spoofed biometric data during verification.
O.Enrol	FIA_MBE_EXT.1	This SFR supports the objective by providing a method for enroling a user for authentication.
	FIA_MBE_EXT.2	This SFR supports the objective by requiring the TSF to enforce a minimum quality standard on the biometric data used for enrolment.
	FIA_MBE_EXT.3 (optional)	This SFR supports the objective by requiring the TSF to detect spoofed biometric data during enrolment.

Objective	Addressed By	Rationale
O.Protection OE.Protection	FDP_RIP.2 (optional)	This SFR supports the objectives by requiring the TOE or its platform to ensure that residual data is purged from the system.
	KPT_KST_EXT.1 (refined from [PP_MD_V3.3])	This SFR supports the objectives by requiring the TOE to prevent the unprotected storage of biometric data.
	KPT_KST_EXT.2 (refined from [PP_MD_V3.3])	This SFR supports the objectives by requiring the TOE to prevent the transmission of biometric data outside the device.
	FPT_BDP_EXT.1	This SFR supports the objectives by requiring the TOE to provide a separate environment for the processing of biometric data which is not available to the main computer operating system.
	FPT_PBT_EXT.1	This SFR supports the objectives by requiring the TOE to protect a user's biometric template with an additional authentication factor.

Chapter 7. 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.

Chapter 8. Consistency Rationale

This section describes consistency rationale between [PP_MD_V3.3] and this PP-Module to show that the unions of Security Problem Definition, objectives, and Security Functional Requirement(SFR)s defined in [PP_MD_V3.3] and this PP-Module do not lead to a contradiction.

8.1. Consistency of TOE Type

When this PP-Module is used to extend [PP_MD_V3.3], 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.

8.2. Consistency of Security Problem Definition

The threats, OSPs and assumptions defined by this PP-Module (see the Security Problem Definition) are consistent with those defined in the [PP_MD_V3.3] as follows:

Table 4. 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_ACCESS (i.e. impersonate the user authentication mechanisms) threat in the [PP_MD_V3.3].
OSP.Enrol	
OSP.Verification_Error	
OSP.Protection	This OSP is specific subsets of the T.PHYSICAL_ACCESS (i.e. direct and possibly destructive access to its storage media (biometric data)) threat in the [PP_MD_V3.3].

8.3. Consistency of Objectives

The objectives for the biometric system and its operational environment are consistent with the [PP_MD_V3.3] 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 [PP_MD_V3.3].
O.Enrol	
O.Protection	This TOE Objective is specific subset of the O.PROTECTED_STORAGE objective in the [PP_MD_V3.3].

Table 6. Consistency Rationale for Environmental Objectives

PP-Module Environmental Objectives	Consistency Rationale
OE.Protection	All Environmental Objectives levied on the operational environment of biometric system (i.e. mobile device) are consistent with security requirements in the [PP_MD_V3.3].

8.4. Consistency of Requirements

The Biometric System (i.e. TSF in this PP-Module) is comprised of biometric capture sensors and firmware/software that provide functions described in this PP-Module TOE design. The Biometric System is invoked by the mobile device as defined in the [PP_MD_V3.3] when user's biometric characteristics is presented to the sensor. The Biometric System creates and stores the template or compares the features with the stored template and returns the verification outcome to the mobile device.

This PP-Module assumes that the mobile device satisfies SFRs defined in the [PP_MD_V3.3] so that the Biometric System can work as specified in this PP-Module. This section explains which SFRs in the [PP_MD_V3.3] are directly relevant to the Biometric System security functionality.

The following rationale identifies several SFRs from [PP_MD_V3.3] that are needed to support Biometric System functionality and explains why the unions of SFRs in the [PP_MD_V3.3] and this PP-Module do not lead to a contradiction.

8.4.1. Relation among SFRs/OEs in the PP_MD_V3.3 and PP-Module

The relation between SFRs defined in the [PP_MD_V3.3] and SFRs in this PP-Module is described below for each security functionality. **Bold SFRs** are those SFRs defined in this PP-Module for the Biometric System and *italicized SFRs* are those defined in [PP_MD_V3.3] for the mobile device.

8.4.1.1. Password authentication

The Password Authentication Factor defined in the [PP_MD_V3.3] is a Non-Biometric Authentication Factor as defined in this PP-Module. Mobile device shall implement the Password Authentication Factor as required by the *FIA_UAU.5.1*. The Biometric Authentication Factor can be used as an alternative authentication mechanism for the user after the initial Password Authentication Factor has been entered to unlock the mobile device.

8.4.1.2. Invocation of the Biometric System

For any modality selected in *FIA_UAU.5.1*, the mobile device shall invoke the Biometric System to unlock the device under the condition specified in *FIA_UAU.6.2*. Mobile device shall also authenticate the user following the rule specified in *FIA_UAU.5.2*.

The Biometric System shall implement a 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. The Biometric System shall also enrol all modalities selected as specified in **FIA_MBE.EXT.1**, to assure

the quality of samples and templates as specified in **FIA_MBV.EXT.2** and **FIA_MBE.EXT.2**. The Biometric System may also prevent use of artificial presentation attack instruments during the biometric enrolment and verification as specified in **FIA_MBE.EXT.3** and **FIA_MBV.EXT.3**.

8.4.1.3. Handling the verification outcome

The mobile device shall take appropriate actions after receiving the verification outcome from the Biometric System 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. The mobile device also shall apply authentication throttling after failed biometric verification, as required by *FIA_TRT_EXT.1.1*.

8.4.1.4. Protection of the Biometric System and its biometric data

The mobile device shall provide the Separate Execution Environment (e.g. restricted operational environment) so the Biometric System can work securely. This Separate Execution Environment guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. This Separate Execution Environment is out of scope of the Biometric System defined in this PP-Module and shall be provided by the mobile device and evaluated based on [PP_MD_V3.3]. However, ST author shall explain how such Separate Execution Environment is provided by the mobile device for the Biometric System, as required by [BIOSD]. The mobile device shall also keep secret any sensitive information regarding the biometric when the mobile device receives the verification outcome from the Biometric System, as required by *FIA_UAU.7.1*, and provide cryptographic support to encrypt or decrypt biometric data as required by *FCS class*. The mobile device shall treat source biometric data and values used in the enrolment or verification process (not the final templates) as keying material and critical security parameters according the *FCS_CKM_EXT.4.2*.

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

However, the Biometric System shall use this Separate Execution Environment correctly to protect biometric data and satisfy the following requirements:

- The Biometric System shall process any plaintext biometric data (e.g. capturing biometric characteristic, creating samples, features and templates) for biometric enrolment and verification within the boundary of the Separate Execution Environment. This implies that:
  - Any part of the Biometric System that processes plaintext biometric data shall be within the boundary of the Separate Execution Environment. For example, the biometric capture sensor shall be configured to be within the boundary of the Separate Execution Environment, so that only the Separate 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 Separate Execution Environment.
  - Plaintext biometric data shall never be accessible from outside the Separate Execution Environment, and any entities outside the Separate Execution Environment can only access the result of process of biometric data (e.g. success or failure of biometric verification)

through the interface provided by the Biometric System.

- The Biometric System shall not transmit any plaintext biometric data outside of the Separate Execution Environment.

If the Biometric System stores any part of the biometric data outside the Separate Execution Environment, the Biometric System shall protect such data so that any entities running outside the Separate Execution Environment can not get access to any plaintext biometric data. ST author shall explain what biometric data resides outside the Separate Execution Environment as required by [BIOSD] and if no data resides outside the environment, requirements below is implicitly satisfied.

- The Biometric System shall not store any plaintext biometric data outside the Separate Execution Environment. As described in this PP-Module Section TOE design, the Biometric System can store templates in the enrolment database. The Biometric System shall encrypt templates using cryptographic service provided by the mobile device within the Separate Execution Environment before storing them in the database, even if the mobile device storage itself is encrypted by the mobile device.
- The Biometric System may overwrite encrypted biometric data in the storage when no longer needed. For example, the Biometric System may overwrite an encrypted template when it is revoked. This is an optional requirement.

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

- The Biometric System 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_KST_EXT.1** and **FPT_KST_EXT.2** in Security Functional Requirements and **FDP_RIP.2** in Optional Requirements in this PP-Module.

8.4.1.5. Management of the Biometric System configuration

The 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.6.2*.

The [BIOPP-Module] assumes that above requirements are satisfied by the TOE environment as defined in OE.Protection.

Chapter 9. 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.

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

Chapter 10. Optional Requirements

This section comprises requirements that can be included in the ST, but are not mandatory for a TOE to claim conformance to this PP-Module.

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.

10.1. Identification and Authentication (FIA)

10.1.1. 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 enroled.

10.1.2. FIA_MBV_EXT.3 Presentation attack detection for biometric verification

FIA_MBV_EXT.3.1

The TSF shall provide a biometric verification mechanism with the IAPAR not exceeding [**assignment**: *value equal to or less than 15% (15:100)*] to prevent use of artificial presentation attack instruments from being successfully verified.

Application Note 14

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

10.2. User data protection (FDP)

10.2.1. 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 15

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

Chapter 11. 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].)

11.1. Identification and Authentication (FIA)

11.1.1. Biometric enrolment (FIA_MBE_EXT)

11.1.1.1. 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.

11.1.1.2. Component levelling

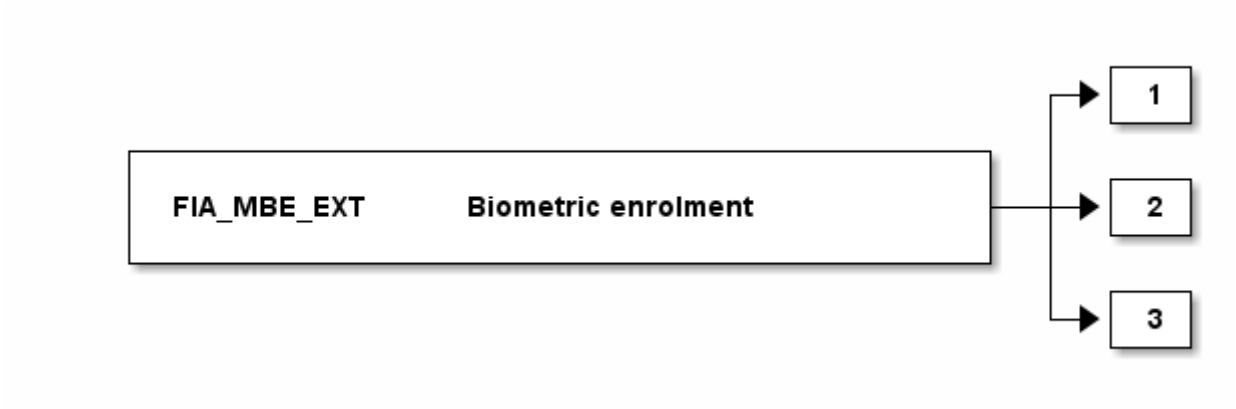

Figure 3. Component levelling

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 detect and prevent presentation attacks during the biometric enrolment.

11.1.1.3. Management: FIA_MBE_EXT.1

There are no management activities foreseen.

11.1.1.4. 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.

11.1.1.5. 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.

11.1.1.6. 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 Base-PP/ST:

a) Basic: Success or failure of the biometric enrolment

11.1.1.7. Audit: FIA_MBE_EXT.3

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

a) Basic: Detection of presentation attacks

11.1.1.8. 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.

11.1.1.9. 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 only use biometric samples of sufficient quality for enrolment. Sufficiency of sample data shall be determined by measuring sample with [**selection**: [[**assignment**: *quality metric standard*] using a threshold of [**assignment**: *quality metric threshold*]], [**assignment**: *developer defined quality assessment method*]].

11.1.1.10. 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 enroled.

11.1.2. Biometric verification (FIA_MBV_EXT)

11.1.2.1. 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.

11.1.2.2. Component levelling

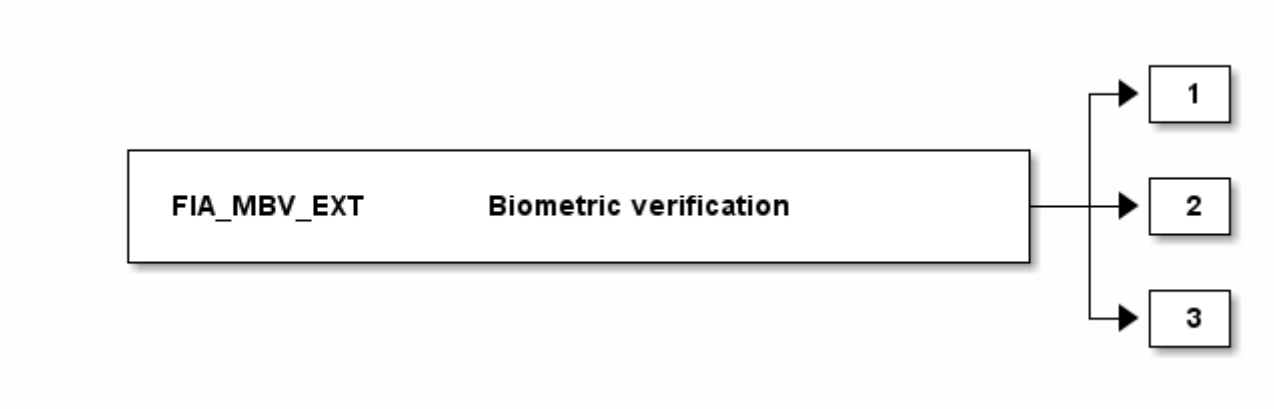

Figure 4. Component levelling

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 detect and prevent presentation attacks during the biometric verification.

11.1.2.3. 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.

11.1.2.4. 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.

11.1.2.5. 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.

11.1.2.6. 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 Base-PP/ST:

a) Basic: Success or failure of the biometric verification

11.1.2.7. Audit: FIA_MBV_EXT.3

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

a) Basic: Detection of presentation attacks

11.1.2.8. 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:** *eye, face, fingerprint, vein*].

FIA_MBV_EXT.1.2

The TSF shall provide a biometric verification mechanism with the [**selection**: *FMR, FAR*] not exceeding [**assignment**: *value equal to or less than 0.01% (1:10^4)*] for the upper bound of [**assignment**: *value equal to or greater than 80%*] confidence interval and, [**selection**: *FNMR, FRR*] not exceeding [**assignment**: *value equal to or less than 5% (5:100)*] for the upper bound of [**assignment**: *value equal to or greater than 80%*] confidence interval.

11.1.2.9. 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 biometric samples of sufficient quality for verification. Sufficiency of sample data shall be determined by measuring sample with [**selection**: [[**assignment**: *quality metric standard*] using a threshold of [**assignment**: *quality metric threshold*]], [**assignment**: *developer defined quality assessment method*]].

11.1.2.10. 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 provide a biometric verification mechanism with the IAPAR not exceeding [**assignment**: *value equal to or less than 15% (15:100)*] to prevent use of artificial presentation attack instruments from being successfully verified.

11.2. Protection of the TSF (FPT)

11.2.1. Biometric data processing (FPT_BDP_EXT)

11.2.1.1. 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.

11.2.1.2. Component levelling

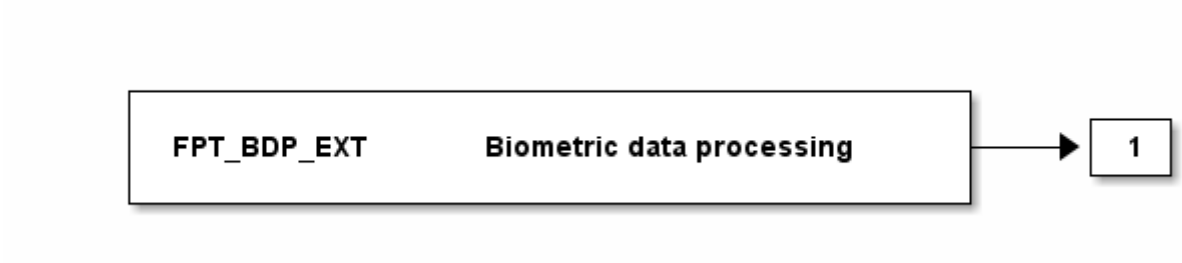

Figure 5. Component levelling

FPT_BDP_EXT.1 Biometric data processing requires the TSF to process plaintext biometric data within the in a separate execution environment and to protect the internal transmission of the biometric data from the main computer operating system.

11.2.1.3. Management: FPT_BDP_EXT.1

There are no management activities foreseen.

11.2.1.4. Audit: FPT_BDP_EXT.1

There are no auditable events foreseen.

11.2.1.5. FPT_BDP_EXT.1 Biometric data processing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_BDP_EXT.1.1

Processing of plaintext biometric data used to generate templates and perform sample matching shall be hardware-isolated from the main computer operating system on the TSF in runtime.

FPT_BDP_EXT.1.2

Transmission of plaintext biometric data between the capture sensor and the SEE shall be isolated from the main computer operating system on the TSF in runtime.

11.2.2. Protection of biometric template (FPT_PBT_EXT)

Family Behaviour

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

11.2.2.1. Component levelling

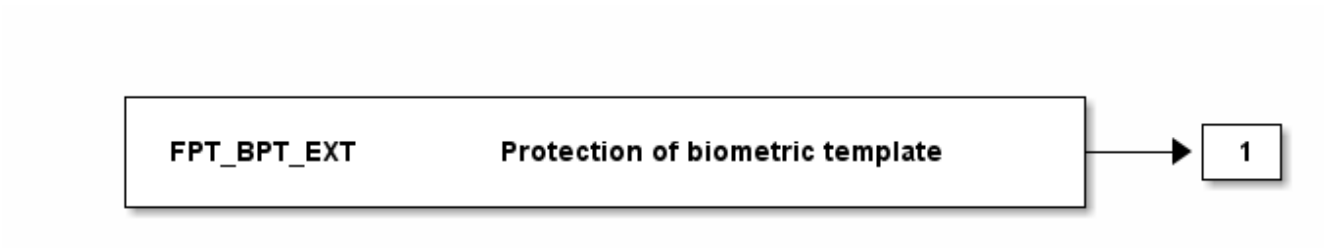

Figure 6. Component levelling

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.

11.2.2.2. 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*]].

Chapter 12. Biometrics Management Description (BMD)

The documentation of the product's biometric functionality and performance should be detailed enough that, after reading, the evaluator will thoroughly understand the product's biometric functionality and performance. As some of this information may be considered confidential to the developer yet still necessary for understanding, this documentation is not required to be part of the TSS and can be submitted as a separate document marked as developer proprietary.

Whether to use the BMD for any information is up to the developer. When used, a non-proprietary summary of the contents of the BMD must be provided in the TSS.