PP-Configuration for Protection Profile for Mobile Device Fundamentals and collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [CFG-MDF-BIO]

Version 0.99, May 11, 2020

Table of Contents

Acknowledgements

This PP-Configuration 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. Introduction

The purpose of a PP-Configuration is to define a Target of Evaluation (TOE) that combines Protection Profiles (PPs) and PP-Modules for various technology types into a single configuration that can be evaluated as a whole. The scope includes the definition of the configuration of a mobile device (a computer in the terms of the PP-Module) that has biometric enrolment and verification capability. The TOE will be defined by a combination of the components described in PP-Configuration Components Statement.

Chapter 2. PP-Configuration Reference

This PP-Configuration is identified as follows:

- PP-Configuration for Protection Profile for Mobile Device Fundamentals and collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - version 0.99, May 11, 2020 - [CFG-MDF-BIO]

Chapter 3. PP-Configuration Components Statement

This PP-Configuration includes the following components:

- base PP: Protection Profile for Mobile Device Fundamentals, PP_MD_V3.3
- PP-Module: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module]

Chapter 4. TOE overview

TOE type, major security features, expected usage of the TOE and non-TOE hardware, software and/or firmware required by the TOE is described in the [PP_MD_V3.3] and [BIOPP-Module].

Chapter 5. Consistency Rationale

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

5.1. Consistency of TOE Type

When the [BIOPP-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.

5.2. Consistency of Security Problem Definition

The threats, OSPs and assumptions defined by the [BIOPP-Module] (see the Sections: Threats, Organizational Security Policies and Assumptions) are consistent with those defined in the [PP_MD_V3.3] as follows:

Table 1. 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].

Table 2. Consistency Rationale for Assumptions

PP-Module Assumptions	**Consistency Rationale**
A.Alternative	All assumptions levied on the operational environment of biometric system (i.e. mobile device) are consistent with security requirements in the [PP_MD_V3.3].
A.Authentication	
A.User	

5.3. 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 3. 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 4. Consistency Rationale for Environmental Objectives

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

5.4. Consistency of Requirements

The Biometric System (i.e. TSF in the [BIOPP-Module]) is comprised of biometric capture sensors and firmware/software that provide functions described in the [BIOPP-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.

The [BIOPP-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 the [BIOPP-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 [BIOPP-Module] do not lead to a contradiction.

5.4.1. Relation among SFRs/OEs in the PP_MD_V3.3 and BIOPP-Module

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

5.4.1.1. Password authentication

The Password Authentication Factor defined in the [PP_MD_V3.3] is a Non-Biometric Authentication Factor as defined in the [BIOPP-Module]. Mobile device shall implement the Password Authentication Factor as required by the *FIA_UAU.5.1*. This password authentication is used as an alternative authentication mechanism when the user is rejected by the biometric verification.

The [BIOPP-Module] assumes that above requirements are satisfied by the mobile device as defined in OE.Alternative.

5.4.1.2. 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 [BIOPP-Module] assumes that above requirements are satisfied by the mobile device as defined in OE.Authentication.

The Biometric System shall implement a biometric verification mechanism that satisfies SFRs defined in the [BIOPP-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**.

5.4.1.3. 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*.

The [BIOPP-Module] assumes that above requirements are satisfied by the mobile device as defined in OE.Authentication.

5.4.1.4. Protection of the Biometric System and its biometric data

The mobile device shall provide the Secure Execution Environment (e.g. restricted operational environment) so that Biometric System can work securely. This Secure Execution Environment guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. This Secure Execution Environment is out of scope of the Biometric System defined in the [BIOPP-Module] and shall be provided by the mobile device and evaluated based on [PP_MD_V3.3]. However, ST author shall explain how such Secure 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*.

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

However, the Biometric System shall use this Secure 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 Secure Execution Environment. This implies that:
  - Any part of the Biometric System that processes plaintext biometric data shall be within the boundary of the Secure Execution Environment. For example, the biometric capture sensor shall be configured to be within the boundary of the Secure Execution Environment, so that only the Secure Execution Environment can access to the sensor and the data captured. Any software modules that process plaintext biometric data shall run within the boundary of the Secure Execution Environment.
  - Plaintext biometric data shall never be accessible from outside the Secure Execution Environment, and any entities outside the Secure Execution Environment can only access the result of process of biometric data (e.g. success or failure of biometric verification) through the interface provided by the Biometric System.
- The Biometric System shall not transmit any plaintext biometric data outside of the Secure Execution Environment.

If the Biometric System stores any part of the biometric data outside the Secure Execution Environment, the Biometric System shall protect such data so that any entities running outside the Secure Execution Environment can not get access to any plaintext biometric data. ST author shall explain what biometric data resides outside the Secure 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 Secure Execution Environment. As described in the [BIOPP-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 Secure 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_BDP_EXT.2** and **FPT_PBT_EXT.3** in Security Functional Requirements and **FDP_RIP.2** in Optional Requirements in the [BIOPP-Module].

5.4.1.5. 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 6. Conformance claim and conformance statement

6.1. Common Criteria Conformance claim

This PP-Configuration, [PP_MD_V3.3] and [BIOPP-Module] are conformant to Common Criteria Version 3.1, Revision 5.

6.2. The conformance type

To be conformant to this PP-Configuration, an ST must demonstrate Exact Conformance.

6.3. The Assurance package conformance claim

In order to evaluate a TOE that claims conformance to this PP-Configuration, the evaluator shall evaluate the TOE against the following SARs that are defined in the [PP_MD_V3.3]:

Table 5. Assurance Components

Assurance Class	**Assurance Components**
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives for the Operational Environment (ASE_OBJ.1)
	Stated Security Requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
	Timely Security Updates (ALC_TSU_EXT)
Tests (ATE)	Independent testing - conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

Note that to fully evaluate the TOE, these SARs shall be applied to the entire TSF and not just the portions described by [PP_MD_V3.3] where the SARs are defined.

6.4. Evaluation methods/activities references statement

[PP_MD_V3.3] and [BIOSD] define Evaluation Activities for how to evaluate individual SFRs as they relate to the SARs for ASE_TSS.1, AGD_OPE.1, and ATE_IND.1. If optional requirement FDP_RIP.2 is selected in the [BIOPP-Module], the Evaluation Activities for FCS_CKM_EXT.4 in [PP_MD_V3.3] can be applied to FDP_RIP.2.

[BIOPP-Module] does not define any SARs beyond those defined within [PP_MD_V3.3] to which it can claim conformance. It is important to note that the TOE that is evaluated against [BIOPP-Module] is inherently evaluated against [PP_MD_V3.3] as well. This means that EAs in Section 5.2 **Security Assurance Requirements** in [PP_MD_V3.3] should also applied to [BIOPP-Module] with additional application notes or EAs defined in the following Sections.

6.4.1. Class ASE: Security Target

[PP_MD_V3.3] does not define any EAs and there is no additional EAs for [BIOPP-Module].

6.4.2. Class ADV: Development

Same EA defined in [PP_MD_V3.3] should also be applied to [BIOPP-Module].

6.4.3. Class AGD: Guidance Documentation

The evaluator shall take the following additional application notes into account to perform EAs defined in [PP_MD_V3.3].

6.4.3.1. Application note for EA of AGD_OPE.1

[BIOPP-Module] defines the assumptions for the mobile device that is the operational environment of the biometric system. These assumptions are implicitly satisfied if the mobile device is successfully evaluated based on [PP_MD_V3.3] and the operational guidance does not need to describe the security measures to be followed in order to fulfil the security objectives for the operational environment derived from those assumptions.

There is additional application note related to EAs for FIA_MBV_EXT.3 in Section 9.3.2 [Additional application notes for AGD Class] in [BIOSD]. The evaluator shall also follow this note depending on the result of the penetration testing for PAD.

6.4.3.2. Application note for EA of AGD_PRE.1

[BIOPP-Module] supposes that the biometric system is fully integrated into the mobile device and the preparative procedures are unnecessary for [BIOPP-Module]. Therefore, AGD_PRE.1 deems satisfied for [BIOPP-Module].

6.4.4. Class ALC: Life-cycle Support

The evaluator shall take the following additional application notes into account to perform EAs

defined in [PP_MD_V3.3] for [BIOPP-Module]. There is no application note for EA for ALC_CMS.1 and ALC_TSU_EXT.

6.4.4.1. Application note for EA of ALC_CMC.1

[BIOPP-Module] is intended to be used with [PP_MD_V3.3] and reference for the mobile device can be used as the TOE (mobile device + biometric system) reference only if the reference for the mobile device also uniquely identifies the biometric system embedded in the mobile device.

6.4.5. Class ATE: Tests

The evaluator shall take the following additional application notes into account to perform EAs defined in [PP_MD_V3.3] for [BIOPP-Module].

6.4.5.1. Application note for EA of ATE_IND.1

Same EA should be applied to [BIOPP-Module] except optional requirement FIA_MBE_EXT.3 (**Presentation attack detection for biometric enrolment**) and FIA_MBV_EXT.3 (**Presentation attack detection for biometric verification**). The evaluator shall perform EAs defined in Section 6 [Evaluation Activities for PAD testing] in [BIOSD] for FIA_MBE_EXT.3 and FIA_MBV_EXT.3.

6.4.6. Class AVA: Vulnerability Assessment

The evaluator shall take the following additional application notes into account to perform EAs defined in [PP_MD_V3.3] for [BIOPP-Module].

6.4.6.1. Application note for EA of AVA_VAN.1

Same EA should be applied to [BIOPP-Module] except optional requirement FIA_MBE_EXT.3 (**Presentation attack detection for biometric enrolment**) and FIA_MBV_EXT.3 (**Presentation attack detection for biometric verification**). The evaluator shall perform EAs defined in Section 6 [Evaluation Activities for PAD testing] in [BIOSD] for FIA_MBE_EXT.3 and FIA_MBV_EXT.3.

In evaluating this PP-Configuration, the evaluator shall ensure that all Evaluation Activities for SFRs and SARs are evaluated as part of satisfying the required SARs.

Chapter 7. Related Documents

Common Criteria[1]

[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.

Protection Profiles

[PP_MD_V3.3]	Protection Profile for Mobile Device Fundamentals, Version:3.3
[BIOPP-Module]	collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -, May 11, 2020, Version 1.0 - [BIOPP-Module]
[BIOSD]	Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -, May 11, 2020, Version 1.0 - [BIOSD]

[1] For details see http://www.commoncriteriaportal.org/

Chapter 8. Revision History

Table 6. Revision history

Version	Date	Description
0.8	31 Jan, 2019	First draft for review
0.9	August 5, 2019	Update from Public Review Draft 1
0.91	December 5, 2019	Update to make PAD optional
0.92	December 20, 2019	Public Review Draft 2
0.95	March 13, 2020	Proposed Release
0.99	May 11, 2020	Public Release (requires PP_MD_V3.3 release to move to v1.0)