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 1.1, September 12, 2022

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 Chapter 3, *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 - [CFG-MDF-BIO], September 12, 2022, Version 1.1

Chapter 3. PP-Configuration Components Statement

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Mobile Device Fundamentals, September 12, 2022, Version 3.3. [PP_MDF]
- PP-Module: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], September 12, 2022, Version 1.1

Chapter 4. Conformance claim and conformance statement

4.1. Common Criteria Conformance claim

This PP-Configuration, [PP_MDF] and [MOD_BIO_V1.0] are conformant to Common Criteria Version 3.1, Revision 5.

4.2. The conformance type

To be conformant to this PP-Configuration, an ST must demonstrate Exact Conformance, as defined by [addenda].

4.3. 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_MDF]:

Table 1. 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.1)
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_MDF] where the SARs are defined.

4.4. Presentation Attack Detection (PAD) conformance

In order to evaluate a TOE that claims conformance to the Presentation Attack Detection (PAD) requirements, the evaluator shall evaluate the TOE using the tests defined in the [Toolbox]. PAD conformance is not mandatory for a TOE under evaluation.

Chapter 5. 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_MDF]	Protection Profile for Mobile Device Fundamentals, September 12, 2022, Version 3.3
[MOD_BIO_V1.0]	collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], September 12, 2022, Version 1.1
[BIOSD]	Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOSD], September 12, 2022, Version 1.1
[Toolbox]	Toolbox Overview, September 12, 2022, Version 1.1

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

Chapter 6. Revision History

Table 2. 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_MDF_V3.3 release to move to v1.0)
1.1	September 12, 2022	Version 1.1