PP-Configuration for Protection Profile for Mobile Device Fundamentals and collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device -

Version 0.8, 2019-05-01

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.

1. Introduction

1.1. Overview

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 that has biometric enrolment and verification capability. The TOE will be defined by a combination of the components described in section 1.3.

1.2. PP-Configuration Reference

This PP-Configuration is identified as follows:

- PP-Configuration for Protection Profile for Mobile Device Fundamentals and collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device - version 0.8, May 01, 2019
- As a shorthand reference, it can be identified as "PPC+MDF+BIO+01"

1.3. PP-Configuration Components Statement

This PP-Configuration includes the following components:

- base PP: Protection Profile for Mobile Device Fundamentals [MDFPP]
- PP-Module: collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device - [BIOcPP Module].

2. Conformance Claims

2.1. CC Conformance

Conformance Statement

To be conformant to this PP-Configuration, an ST must demonstrate Exact Conformance, a subset of Strict Conformance as defined in [MDFPP].

The ST must include all components in the base PP that are:

- Unconditional (which are always required)
- Selection-based (which are required when certain selections are chosen in the unconditional requirements)

and may include components that are

- Optional
- Objective.

The same conditions apply to [BIOcPP Module] that is included as part of this PP-Configuration.

CC Conformance Claims

This PP-Configuration, [MDFPP] and [BIOcPP Module] are conformant to Common Criteria Version 3.1, Revision 5.

2.2. SAR Statement

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 [MDFPP]:

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)
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 [MDFPP] where the SARs are defined.

In addition to this, both [MDFPP] and [BIOcPP Module] 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. [MDFPP] and [BIOcPP Module] also provide Evaluation Activities for the SARs. 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.

2.3. Related Documents

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

[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

[MDFPP]	Protection Profile for Mobile Device Fundamentals, Version:3.2
[BIOcPP Module]	collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device -, January 31, Version 0.8, 2019

2.4. Revision History

Version	Date	Description
0.8	31 Jan, 2019	First draft for review