collaborative Protection Profile for *Some Product*

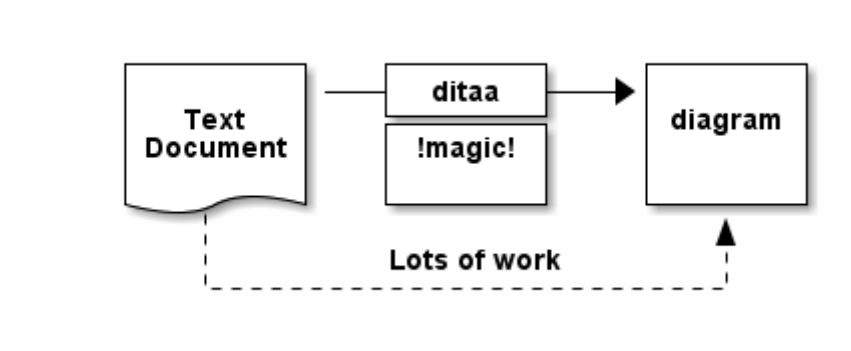
Version 0.1, 2019-04-04

Table of Contents

1. Acknowledgements

This collaborative Protection Profile (cPP) was developed by the *my iTC name* international Technical Community (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 Protection Profile Module (cPP Module) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for *some environment*. The Evaluation activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this cPP Module, are described in Supporting Documents.

2.2. Scope of Document

The scope of the cPP Module within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation. In particular, a cPP 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 cPP Module are developers, CC consumers, system integrators, evaluators and schemes.

Although the cPP Module and SD may contain minor editorial errors, the cPP Module is recognized as living document and the iTC is dedicated to ongoing updates and revisions. Please report any issues to the *my* 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.

2.5. Glossary

For the purpose of this cPP Module, the following terms and definitions given in *some specific references* apply. If the same terms and definitions are given in those references, terms and definitions that fit the context of this cPP Module take precedence.

Attempt

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

2.6. Revision History

Table 1. Revision history

Version	Date	Description
0.1	April 4, 2019	Preliminary draft
0.2		

3. PP Introduction

3.1. PP Reference Identification

- PP Reference: collaborative Protection Profile for _Some Product_
- PP Version: 0.1
- PP Date: 2019-04-04

3.2. TOE Overview

Some intro stuff here

3.3. TOE Design

Some design stuff here (maybe an image or two)

3.4. TOE Use Case

If you are defining use cases (such as specific use scenarios that may have unique requirement selections), put that here.

3.4.1. USE CASE 1: first use case

3.4.2. USE CASE 2: second use case

4. CC Conformance Claims

As defined by the references [CC1], [CC2] and [CC3], this cPP Module:

- conforms to the requirements of Common Criteria v3.1, Revision 5,
- is Part 2 extended,
- does not claim conformance to any other security functional requirement packages.

In order to be conformant to this cPP Module, a ST shall demonstrate Exact Conformance. Exact Conformance, as a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the SFRs in Security Functional Requirements (these are the mandatory SFRs) of this cPP Module, and potentially SFRs from Consistency Rationale (these are selection-based SFRs) and Selection-Based Requirements (these are optional SFRs) of this cPP Module. While iteration is allowed, no additional requirements (from the CC parts 2 or 3, or definitions of extended components not already included in this cPP Module) are allowed to be included in the ST. Further, no SFRs in Security Functional Requirements of this cPP Module are allowed to be omitted.

5. 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.

5.1. Threats

5.2. Organizational Security Policies

5.3. Assumptions

6. Security Objectives

6.1. Security Objectives for the TOE

6.2. Security Objectives for the Operational Environment

6.3. 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

7. Security Functional Requirements

7.1. 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** indicates additional text provided as a refinement.
- **[Bold text within square brackets]** indicates the completion of an assignment.
- [text within square brackets] indicates the completion of a selection.
- Number in parentheses after SFR name, e.g. (1) indicates the completion of an iteration.

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

7.2. Identification and Authentication (FIA)

8. Security Assurance Requirements

9. Consistency Rationale

Table 3. Consistency Rationale for threats and OSPs

cPP Module Threats/OSPs	Consistency Rationale

Table 4. Consistency Rationale for Assumptions

cPP Module Assumptions	Consistency Rationale

9.1. Consistency of Objectives

The objectives for the biometric system and its operational environment are consistent with the [MDFPP] based on the following rationale:

Table 5. Consistency Rationale for TOE Objectives

cPP Module TOE Objectives	Consistency Rationale

Table 6. Consistency Rationale for Environmental Objectives

cPP Module Environmental Objectives	Consistency Rationale

9.2. Consistency of Requirements

10. Selection-Based Requirements

As indicated in the introduction to this cPP Module, the baseline requirements (those that shal be performed by the TOE) are contained in Security Functional Requirements. Additionally, there are two other types of requirements specified in Consistency Rationale and Selection-Based Requirements.

The first type (in this chapter) comprises requirements based on selections in other SFRs from the cPP Module: if certain selections are made, then additional requirements in this chapter will need to be included in the body of the ST.

The second type (in this chapter) comprises requirements that can be included in the ST, but are not mandatory for a TOE to claim conformance to this cPP Module.

11. Optional Requirements

ST authors are free to choose none, some or all SFRs defined in this chapter. Just the fact that a product supports a certain functionality does not mandate to add any SFR defined in this chapter.

12. Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the cPP Module, including those used in Consistency Rationale and Selection-Based Requirements .

(Note: formatting conventions for selections and assignments in this chapter are those in [CC2].)

13. Annex A Consistency Rationale between this cPP Module and *some other* PP

13.1. Overview

This Annex describes consistency rationale between this cPP Module and *some other*.