Biometric cPP

Version: 3.1

2017-06-16

tbd

Revision History

Version	Date	Comment
0.1	2016-06-24	Initial Version

Contents

1. Introduction

1.1 Objectives of Document

This document comprises the Security Problem Definition for the biometric iTC. The iTC currently discusses three different TOE that are all covered by the content in this document, namely:

- A TOE for presentation attack detection (PAD) only (also referred to as TOE.PAD),
- A TOE for biometric verification only (also referred to TOE.BIO),
- An integrated solution with PAD and biometric verification (also referred to as TOE.INT).

This document contains the description for TOE.BIO. The Security Problem Definition comprises:

- A description of the external parties that interact with the TOE,
- A description of the assets to be protected by the TOE,
- A list of assumptions describing the intended environment of the TOE,
- A list of threats posed against the TOE,
- Organizational Security Policy (OSP) which is a set of rules, practices, and procedures imposed by an organization to address its security needs..

The Security Problem Definition defines the minimum set that applies to all possible architectures of the TOE. However, certain architectures of the TOE may face additional threats or OSPs and will also have to implement additional functionality. As an example: A biometric algorithm may generate suitable audit events to be recorded by its environment but has – by itself – no mean to record or handle the events. A complete biometric system on the other hand, has the functionality to store and handle audit events. This Protection Profile chooses the following approach to address this situation:

- The requirements defined within the Security Problem Definition (and later on within the Objectives/SFR chapter) are to be met by every TOE, regardless of its architecture.)
- Chapter TBD defines additional functional packages that define additional requirements for certain architectures of a TOE.
- If a TOE meets the architecture of a functional package, the ST author shall include all requirements from that functional package to their ST.

1.2 Scope of Document

The scope of the Protection Profile within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC] . In particular, a defines the IT security requirements of a generic type of and specifies the functional and assurance security measures to be offered by that to meet stated requirements [CC] .

1.3 Intended Readership

The target audiences of this are biometric Device developers, consumers, evaluators and schemes.

1.4 Glossary

PAD	Presentation Attack Detection.

1.5 External Parties

The following list comprises the external parties that may interact with the TOE.

Administrator

The TOE administrator is authorized and responsible to perform administrative TOE operations and able to use the administrative functions of the TOE. The administrator is also responsible for the installation and maintenance of the TOE. Depending on the concrete implementation of the TOE there may be more than one administrator and consequently also more than one administrative role. It is also possible that the role of the administrator is held by a user of the TOE.

User

A person who uses a biometric system to get enrolled or verified.

Attacker

An attacker is any individual who is attempting to subvert the operation of the TOE.

1.6 Assets

The following table comprises the assets that are to be protected by the TOE

Access

A biometric authentication system is used to control access to a physical or logical portal. The access to this portal (or the decision about granting access to be precise) is a primary asset for every biometric authentication

PAD result

If the TOE implements a PAD system, the decision on whether an attempt with the TOE is considered being a Presentation Attack is a primary asset.

TSF Data

All data for the operation of the TOE upon which the enforcement of the security mechanisms relies.

1.7 TOE Overview

tbd

1.8 TOE Usage

tbd

2. CC Conformance

As defined by the references [CC] , this conforms to the requirements of Common Criteria v3.1, Revision 5. The methodology applied for the evaluation is defined in [CEM] .

This satisfies the following Assurance Families: tbd

3. Security Problem Definition

3.1 Threats

The following table comprises the threats that are directed against the TOE.

T.Casual_Attack
An attacker may attempt to impersonated as a legitimate user without being enrolled in the system themselves. In order to perform the attack, the attacker only uses their own biometric characteristic (in form of a zero-effort-attack)

T.PA_Enrolment
An attacker may attempt to get impersonated as another user during enrolment. In order to perform the attack, the attacker uses artificial biometric characteristics, carrying the biometric characteristic of the attacked user (as so called Presentation Attack)

T.PA_Verification
An attacker may attempt to get impersonated (during verification process) as a legitimate user without being enrolled in the system themselves. In order to perform the attack, the attacker uses artificial biometric characteristics, carrying the biometric characteristic of the attacked user (as so called Presentation Attack)

T.General
An attacker can carry out any kind of logical or physical attacks that do not exceed the attack potential and that are compliant with A.Environment as defined in the cPP in order to disguise his/her own identity during the enrolment or verification process or for the sake of impersonation. More specifically, an attacker may try to modify TSF data (e.g. settings for the biometric verification process) in order to impact the normal operation of the TOE.

T.Residual
An attacker may try to take advantage of unprotected residual security relevant data (e.g. biometric data and settings) during a user's session or from a previous, already authenticated user. In this way the attacker tries to get access to the security relevant settings of the TOE. This threat covers several scenarios including: - An attacker takes advantage of the verification memory content (e.g. by reading the memory content, cache or relevant temporary data) using a flaw in a user visible interface of the TOE. - An attacker may take advantage of residual images at the capture device. These are likely to be limited to cases where physical contact with the biometric capture device is necessary for the biometric modality (e.g. fingerprints)

T.Roles
An enrolled and authenticated user may try to exceed their privileges. This specifically addresses the cases where an authorized user tries to get administrator privileges in order to modify TSF data.

*

3.2 Assumptions

The following table comprises the assets that assumptions about the intended environment of the TOE.

A.Admin
It is assumed that the administrator of the TOE is well trained and non-hostile. Non-hostile specifically means that the administrator does not become an attacker nor does the administrator give relevant information to attackers. The administrator is responsible to accompany the TOE installation and oversees the system requirements regarding the TOE as well as the TOE settings and requirements.

A.Environment
The TOE is assumed to be used in a semi-controlled and observable environment (i.e. attacks that require extensive time or extensive access to the TOE or the use of complex tools (in the sense of conspicuous tools) are considered impractical during exploitation phase). This assumption also includes the protection of any parameters used by the TOE.

A.Comm
It is assumed that the communication between the components of the biometric product is adequately protected against manipulation and eavesdropping of information.

A.Fallback
It is assumed that a fall-back mechanism as a complement to the TOE is available that reaches at least the same level of security as the biometric verification system does. This fall-back system is used in cases where an authorized user is rejected by the biometric verification system (False Rejection).

A.Bio
The biometric system protected by the TOE ensures that all threats that are not related to presentation attacks are appropriately handled. Further, the biometric system ensures that the functionality of the TOE is invoked/used in order to protect the biometric system against presentation attacks. It is also assumed that the biometric sample that is acquired by the capture devices belongs to the sample that is used for presentation attack detection.The PAD system addressed in this Protection Profile is a protection mechanism against presentation attacks.

A.PAD
It is assumed that the biometric system is protected against Presentation Attacks according to PP [bioCPP].

3.3 Organizational Security Policies

The following list comprises the OSP that the TOE shall comply with.

OSP.ENROL
The TOE shall implement the functionality to enrol users. The TOE shall ensure that enrolment records are of sufficient quality in order to meet the requirements on recognition performance. Start of Enrolment shall only be possible after authorization of an authorized administrator.

OSP.Verifcation_Error
The TOE shall meet relevant criteria for its security relevant error rates for biometric verification (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)).

OSP.PAD_Error
The TOE shall meet relevant criteria for its security relevant error rates for PAD.

OSP.TrialLimit
Impostors must be prevented from gaining access to the portal by making repeated verification attempts using one or more claimed user IDs. Therefore the TOE in cooperation with its environment shall be able to limit the maximum number of unsuccessful verification attempts.

OSP.Audit
In order to

- generate statistics that can be used to adjust the parameters for better quality (maintenance)
- trace modification and
- trace possible attacks

the TOE shall generate security-relevant audit events.

OSP.Residual
The TOE shall erase all residual security-relevant data once they are redundant.. This specifically includes (but is not limited to) all information left after enrolment, verification or PAD processing.

4. Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the Mobile Device are defined as follows.

O.BIO_VERIFICATION
The TOE shall provide a biometric verification mechanism to ensure access to a portal with an adequate reliability. The TOE shall meet relevant criteria for its security relevant error rates for biometric verification (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)). An “Exact match” should not be counted as a positive verification as it may be a replay attempt.

Addressed by:

O.PAD
The TOE shall detect whether a presentation is an presentation attack is or a bona fide presentation. The evidence may be extracted from the data provided by the same sensor that is used to acquire the biometric characteristic for recognition (by the biometric system in the environment), or it may be retrieved using sensors which are solely dedicated to PAD.

Addressed by:

O.PAD
The TOE shall detect whether a presentation is an presentation attack is or a bona fide presentation. The evidence may be extracted from the data provided by the same sensor that is used to acquire the biometric characteristic for recognition (by the biometric system in the environment), or it may be retrieved using sensors which are solely dedicated to PAD.

Addressed by:

O.PAD_ENROL
The TOE shall prevent an attacker facilitating a presentation attack from being successfully enrolled,

Addressed by:

O.PAD_VERIFICATION
The TOE shall prevent an attacker facilitating a presentation attack from being successfully verified.

Addressed by:

O.AUDIT
The TOE shall report or record

A use of the central functionality of the TOE and its result Every use of a management function All parameters modified by the management functions

Addressed by: The use of the central functionality of the TOE refers to the use of the PAD functionality in case of TOE.PAD and to the use of the biometric functionality in case of TOE.BIO.Please note that the term “report” in O.Audit does only require the TOE to generate the audit event while it is possible that the storage of the events is done by the environment.

O.ENROL
The TOE shall implement the functionality to enrol users. The TOE shall ensure that enrolment records are of sufficient quality in order to meet the requirements on recognition performance. The TOE shall ensure that start of Enrolment shall only be possible after authorization by an administrator.

Addressed by:

O.RESIDUAL
The TOE shall ensure that no residual or unprotected security relevant data remain in memory or on any sensor after operations are completed.

Addressed by: In case no sensor is part of the TOE, this part of the objective shall be considered fulfilled.

O.MANAGEMENT
The TOE shall provide the necessary management functionality for the modification of security relevant parameters to TOE administrators only. As part of this management functionality the TOE shall only accept secure values for security relevant parameters to ensure the correct operation of the TOE.

Addressed by:

O.PAD_ERROR
The TOE shall meet relevant criteria for its security relevant error rates for PAD

Addressed by: It is the concept of this PP that concrete values for security relevant error rates shall not be defined in the PP/ST. Instead, such concrete values should be defined in the corresponding methodology documents.

O.PROTECTION
The TOE in cooperation with its immediate environment shall provide an adequate level of logical and physical protection in order to ensure the correct operation of the TOE. This specifically concerns the enrolment and verification process. Impostors must be prevented from gaining access to the portal by making repeated verification attempts using one or more claimed user IDs. Therefore the TOE in cooperation with its environment shall be able to limit the maximum number of unsuccessful verification attempts. Also, the TOE − in cooperation with its environment − shall ensure that any TSF data is adequately protected.

Addressed by: The relationship between the TOE and its environment is pretty complex in this point and deserves some further explanation: A.Environment does not pose an absolute protection for the TOE to be provided by the environment. It provides a level of protection, in which complex attacks may not be possible. However, simple and unobstrusive attacks can still be performed. Such attacks are described in T.General and have to be countered by the TOE itself as required by this objective.

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

OE.ADMIN
The administrator of the TOE shall be well trained and non-hostile. Non-hostile specifically means that the administrator does not become an attacker nor does the administrator give relevant information to attackers. The administrator is responsible to witness the TOE installation and oversees the system requirements regarding the TOE.

OE.Environment
The direct environment of the TOE shall be semi-controlled and observable. This specifically means that attacks that require extensive time or extensive access to the TOE or the use of complex tools (in the sense of conspicuous tools) shall be rendered impractical by the environment.

OE.COMM
The direct environment of the TOE shall adequately protect the communication between the components of the biometric product against manipulation and eavesdropping

OE.FALLBACK
The environment shall provide a fall-back mechanism as a complement to the TOE that reaches at least the same level of security as the biometric verification system. This fall-back system is used in cases where an authorized user is rejected by the biometric verification system (False Rejection).

OE.FALLBACK
The biometric system protected by the TOE shall ensure that all threats that are not related to PAD are appropriately handled. Further, the biometric system ensures that the functionality of the TOE is invoked/used in order to protect the biometric system against Presentation Attacks. It is also assumed that the biometric sample that is acquired by the capture devices belongs to the sample that is used for PAD. Note: Compliance to this security objective can be easily shown by providing a certificate for the biometric system in the environment showing that the biometric system fulfils all the requirements from [bioCPP]. The PAD system addressed in this Protection Profile is a protection mechanism against presentation attacks.

OE.PAD
The biometric system shall be protected against Presentation Attacks according to PP [padCPP]. Note: Compliance to this security objective can be shown by providing a Common Criteria certificate for the PAD system in the environment showing that the PAD system fulfils all the requirements from [padCPP]. The biometric system addressed in this Protection Profile serves to authenticate users and does not provide any functionality for PAD.

OE.PAD
The environment shall provide functionality to associate users with roles. This functionality of the environment is an important aspect that contributes to counter threats that include aspects of a role model (like T.Roles). The minimum TOE as defined in this Protection Profile may not have the functionality to distinguish roles for users. For that reason, this functionality is provided by the environment.

OE.AdminAuth
The environment shall provide a secure and non biometric authentication mechanism for the authentication of administrators.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.Casual_Attack	O.BIO_VERIFICATION	The threat T.EAVESDROP is countered by O.BIO_VERIFICATION as this objective requires the TOE to provide a biometric authentication mechanism that is resistant against attacks of this kind.
T.PA_Enrolment	O.PAD, O.PAD_ENROL, O.ENROL	Tbd Tbd tbd
T.PA_Verification	O.BIO_VERIFICATION, O.PAD, O.PAD_VERIFICATION	tbd tbd tbd
T.General	O.PROTECTION	tbd
T.Residual	O.RESIDUAL	tbd
T.Roles	O.MANAGEMENT	tbd
A.Admin	OE.Admin	The assumption A.Admin is covered by the security objective OE.Admin. The assumption and the objective are drafted in a way that the correspondence is obvious.
A.Environment	OE.Environment	The assumption A.Environment is covered by the security objective OE.Environment. The assumption and the objective are drafted in a way that the correspondence is obvious.
A.Comm	OE.Comm	The assumption A.Comm is covered by the security objective OE.Comm. The assumption and the objective are drafted in a way that the correspondence is obvious.
A.Fallback	OE.Fallback	The assumption A.Fallback is covered by the security objective OE.Fallback. The assumption and the objective are drafted in a way that the correspondence is obvious.
A.Bio	OE.Bio	The assumption A.Bio is covered by the security objective OE.Bio. The assumption and the objective are drafted in a way that the correspondence is obvious.
A.PAD	OE.PAD	The assumption A.PAD is covered by the security objective OE.PAD. The assumption and the objective are drafted in a way that the correspondence is obvious.
OSP.ENROL		
OSP.Verifcation_Error		
OSP.PAD_Error		
OSP.TrialLimit		
OSP.Audit		
OSP.Residual		

A. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model , CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
[CEM]	Common Evaluation Methodology for Information Technology Security - Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

B. Acknowledgements

Tbd