Supporting Document Mandatory Technical Document

Evaluation Activities for collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device -

Version 0.3, 2019-05-01

Table of Contents

Foreword

This is a Supporting Document, intended to complement the Common Criteria (CC) version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

Supporting Documents may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the Supporting Document. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

This Supporting Document has been developed by the Biometric Security iTC (BIO-iTC) and is designed to be used to support the evaluations of TOEs against the PP-Module identified in Section 1.1, “Technology Area and Scope of Supporting Document”.

Technical Editor

Biometric Security international Technical Community (BIO-iTC)

(https://www.commoncriteriaportal.org/communities/Bio.cfm)

Revision History

Table 1. Revision history

Version	Date	Description
0.1	March, 2018	Initial release for internal review
0.2	August 2018	Second release for internal review
0.3	May 1, 2019	Third release for internal review

General Purpose

See section 1.1.

Field of special use

This Supporting Document applies to the evaluation of TOEs claiming conformance with the collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device - [BIOPP-Module].

Acknowledgements

This Supporting Document was developed by the Biometric Security international Technical Community with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

1. Introduction

1.1. Technology Area and Scope of Supporting Document

This Supporting Document (SD) defines the Evaluation Activities (EAs) associated with the collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device - [BIOPP-Module] that is intended for use with the following base PP:

Protection Profile for Mobile Device Fundamentals ([MDFPP])

This SD is mandatory for evaluations of TOEs that claim conformance to [BIOPP-Module].

The Biometric Security technical area has a number of specialised aspects, such as those relating to the mobile biometric enrolment and verification, and to the particular ways in which the TOE needs to be assessed across a range of different Presentation Attack Instruments (PAI). This degree of specialisation, and the associations between individual SFRs in [BIOPP-Module], make it important for both efficiency and effectiveness that EAs are given more specific interpretations than those found in the generic CEM activities.

Although EAs are defined mainly for the evaluator to follow, the definitions in this SD aim to provide a common understanding for developers, evaluators and users as to what aspects of the TOE are tested in an evaluation against [BIOPP-Module], and to what depth the testing is carried out. This common understanding in turn contributes to the goal of ensuring that evaluations against [BIOPP-Module] achieve comparable, transparent and repeatable results. In general, the definition of EAs will also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of SFRs, and may identify particular requirements for the content of Security Targets (STs) (especially the TOE Summary Specification (TSS)), AGD guidance, and possibly supplementary information (e.g. for biometric performance testing – see Section 7, “Developer’s performance test document and its assessment strategy”).

1.2. Structure of the Document

EAs can be defined for both SFRs and SARs. These are defined in separate sections of this SD.

If any EA cannot be successfully completed in an evaluation then the overall verdict for the evaluation is a ‘fail’. In rare cases there may be acceptable reasons why an EA may be modified or deemed not applicable for a particular TOE, but this must be agreed with the Certification Body for the evaluation.

In general, if all EAs (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

1.3. Terminology

1.3.1. Glossary

For definitions of standard CC terminology see [CC1]. For definitions of biometrics and mobile device, see [BIOPP-Module] and [MDFPP].

1.3.2. Acronyms

Acronym	Meaning
BAF	Biometric Authentication Factor
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
EA	Evaluation Activity
iTC	International Technical Community
PAI	Presentation Attack Instrument
PP	Protection Profile
SAR	Security Assurance Requirement
SD	Supporting Document
SEE	Secure Execution Environment
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TSFI	TOE Security Functions Interface
TSS	TOE Summary Specification

2. Evaluation Activities for SFRs

2.1. Structure of EAs

All EAs for SFRs defined in this Section include the following items to keep consistency among EAs.

a. Objective of the EA

   Objective defines the goal of the EA. Assessment Strategy describes how the evaluator can achieve this goal in more detail and Pass/Fail criteria defines how the evaluator can determine whether the goal is achieved or not.

b. Dependency

   Where the EA depends on completion of another EA then the dependency and the other EA is also identified here.

c. Tool types required to perform the EA

   If performing the EA requires any tool types in order to complete the EA then these tool types are defined here.

d. Required input from the developer or other entities

   Additional detail is specified here regarding the required format and content of the inputs to the EA.

e. Assessment Strategy

   Assessment Strategy provides guidance and details on how to perform the EA. It includes, as appropriate to the content of the EA;

   1. How to assess the input from the developer or other entities for completeness with respect to the EA
   2. How to make use of any tool types required (potentially including guidance for the calibration or setup of the tools)
   3. Guidance on the steps for performing the EA

f. Pass/Fail criteria

   The evaluator uses these criteria to determine whether the EA has demonstrated that the TOE has met the relevant requirement or that it has failed to meet the relevant requirement.

g. Requirements for reporting

   Specific reporting requirements that support transparency and reproducibility of the Pass/Fail judgement are defined here.

2.2. Justification for EAs for SFRs

EAs in this SD provide specific or more detailed guidance to evaluate the biometric system, however, it is the CEM work units based on which the evaluator shall perform evaluations.

This Section explains how EAs for SFRs are derived from the particular CEM work units identified in Assessment Strategy to show the consistency and compatibility between the CEM work units and EAs in this SD.

Assessment Strategy for ASE_TSS requires the evaluator to examine that the TSS provides sufficient design descriptions and its verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary information will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in [MDFPP] from which SARs of [BIOPP-Module] are inherited.

Assessment Strategy for AGD_OPE/ADV_FSP requires the evaluator to examine that the AGD guidance provides sufficient information for the administrators/users as it pertains to SFRs, its verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Assessment Strategy for ATE_IND requires the evaluator to conduct testing that the iTC has determined that those testing of the TOE in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that derive those EAs are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.3. Identification and Authentication (FIA)

2.3.1. EA for FIA_MBE_EXT.1

2.3.1.1. Objective of the EA

The evaluator shall verify that the TOE enrols a user only after successful authentication of the user by his/her password. Security requirements for the password authentication are defined in [MDFPP] and out of scope of this EA.

2.3.1.2. Dependency

There is no dependency to other EAs defined in this SD.

2.3.1.3. Tool types required to perform the EA

No tool is required for this EA.

2.3.1.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBE_EXT.1 at high level description
b. AGD guidance shall provide clear instructions for a user to enrol him/herself

AGD guidance may include online assistance, prompts or warning provided by the TOE during the enrolment attempt.

2.3.1.5. Assessment Strategy

2.3.1.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS to understand how the TOE enrols a user and examine the AGD guidance to confirm that a user is required to enter his/her valid password before the mobile biometric enrolment.

2.3.1.5.2. Strategy for ATE_IND

The evaluator shall perform the following test to verify that the TOE performs the mobile biometric enrolment correctly.

a. Step 1: The evaluator shall try to enrol him/herself without setting a password and confirm that he/she can’t enrol him/herself.
b. Step 2: The evaluator shall set a password and confirm that he/she can’t enrol him/herself without entering the password correctly beforehand.

2.3.1.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS and AGD guidance
b. Only authenticated users by password can enrol him/herself and any attempts to enrol without the authentication are rejected through the independent testing

2.3.1.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.3.2. EA for FIA_MBE_EXT.2

2.3.2.1. Objective of the EA

Mobile biometric verification performance depends on quality of the template that is compared to the samples presented to the TOE. The evaluator shall examine that the TOE checks the quality of enrolment and authentication templates based on the assessment criteria to verify a user with an adequate reliability.

If the TOE doesn’t create authentication templates, this EA is only applicable to enrolment templates.

The evaluator shall keep in mind that the assessment criteria for different biometric modalities may not be the same. The evaluator shall evaluate each biometric modality separately if the ST author selects multiple biometric modalities in FIA_MBV_EXT.1.1.

2.3.2.2. Dependency

The evaluator shall perform the EA for FIA_MBE_EXT.1 first to confirm the mobile biometric enrolment can be done correctly.

2.3.2.3. Tool types required to perform the EA

Developer shall provide a test platform for the evaluator to conduct the test described in the Assessment Strategy.

2.3.2.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBE_EXT.2 at high level description
b. AGD guidance shall provide clear instructions for a user to enrol him/herself
c. Supplementary information (Assessment criteria for templates) shall describe assessment criteria for creating templates

AGD guidance may include online assistance, prompts or warning provided by the TOE during the enrolment attempt.

2.3.2.5. Assessment Strategy

2.3.2.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

Enrolment templates

The evaluator shall examine the TSS to understand how the TOE generate templates of sufficient quality at enrolment. The evaluator shall also examine the AGD guidance about how the TOE supports a user to enrol him/herself correctly and how the TOE behaves when low quality samples are presented to the TOE.

The evaluator shall examine that “assessment criteria for templates” to check that how the TOE creates the templates based on this assessment criteria. The “assessment criteria for templates” may include;

a. Quality requirements for the biometric sample to ensure that a sufficient amount of distinctive features is available
b. Method to quantify the quality of samples (e.g. method to generate quality score)
c. Assessment criteria to accept the sample of sufficient utility (e.g. compare quality score to quality threshold)
d. Quality standard that the TOE uses to perform the assessment if the TOE follows such standard (e.g. NFIQ for fingerprint)
e. Additional assessment criteria applied to creation of enrolment templates

Authentication templates

If the TOE creates authentication templates, the evaluator shall examine the TSS to understand how the TOE generate sufficient quality of authentication templates.

The evaluator shall examine that the “assessment criteria for templates” to check that how the TOE creates the authenticate templates based on its assessment criteria. The “assessment criteria for templates” may include a) – d) in Section 3.1.1.5.1, “Strategy for ASE_TSS and AGD_OPE/ADV_FSP” and;

f. Additional assessment criteria to applied to creation of authentication templates

2.3.2.5.2. Strategy for ATE_IND

Enrolment templates

The evaluator shall perform the following test to verify that the TOE generates templates of sufficient quality.

The following test requires the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

a. Step 1: The evaluator shall perform mobile biometric enrolment that results in creation of templates that don’t satisfy the assessment criteria described in “assessment criteria for templates” (e.g. presenting biometric samples of low quality)
b. Step 2: The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that the TOE doesn’t create enrolment templates that don’t meet the assessment criteria specified in the “assessment criteria for templates”

Authentication templates

The evaluator shall perform the following test to verify that the TOE generates authentication templates of sufficient quality only if the evaluator judges that creating authentication templates is feasible.

The following test requires the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

a. Step 1: The evaluator shall enrol him/herself
b. Step 2: The evaluator shall present biometric samples repeatedly to trigger the TOE to create authentication templates
c. Step 3: The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that the TOE doesn’t create authentication templates that don’t meet the assessment criteria specified in the “assessment criteria for templates”

2.3.2.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS, AGD guidance and “assessment criteria for templates”
b. The TOE creates only templates that pass the assessment criteria through the independent testing

2.3.2.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.3.3. EA for FIA_MBV_EXT.1

2.3.3.1. Objective of the EA

The evaluator shall verify that the TOE implements the mobile biometric verification mechanism whose error rates is equal or lower than the claimed error rates (i.e. value of FAR/FMR and FRR/FNMR specified in FIA_MBV_EXT.1.2).

The evaluator shall solely rely on the supplementary information (developer's performance test document) to achieve this objective following instruction defined in Assessment Strategy.

[BIOPP-Module] assumes that the mobile biometric verification is not used for the security sensitive services and the TOE operational environment also limits the maximum number of failed verification attempts in succession. Therefore, risk of zero-effort impostor attempts is low and the developer may not follow the statistical method (e.g. Rule of 3 or Rule of 30) to measure the mobile biometric verification performance.

2.3.3.2. Dependency

The evaluator shall perform the EAs for FIA_MBE_EXT.1 and FIA_MBE_EXT.2 first to confirm the mobile biometric enrolment can be done correctly.

2.3.3.3. Tool types required to perform the EA

No tool is required for this EA.

2.3.3.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBV_EXT.1 at high level description

b. AGD guidance shall provide clear instruction for a user to verify him/herself to unlock the mobile device

c. Supplementary information (developer's performance test document) shall describe developer's performance test protocol and result of testing

AGD guidance may include online assistance, prompts or warning provided by the TOE during the verification attempt.

2.3.3.5. Assessment Strategy

2.3.3.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS to understand how the TOE verify a user with his/her biometric characteristics. The evaluator shall also examine the guidance about how the TOE supports a user to verify him/herself correctly and how the TOE behaves when mobile biometric verification is succeeded or failed.

The evaluator shall examine “developer’s performance test document” to verify that the developer conducts the objective and repeatable performance testing. Minimum requirements for conducting performance testing are defined in Section 7, “Developer’s performance test document and its assessment strategy” (Developer’s performance test document and its assessment strategy).

Requirements defined in Section 7, “Developer’s performance test document and its assessment strategy” is based on the ISO/IEC 19795. This standard specifies requirements on performance test protocol, recording and reporting of results based on the best practices developed by relevant organizations. The evaluator shall confirm that “developer’s performance test document” meets all requirements in Section 7, “Developer’s performance test document and its assessment strategy” and seek a rationale if “developer’s performance test document” doesn’t meet any requirements and determine whether the rationale is valid or not.

Finally, the evaluator shall check that the measured error rates (FRR/FAR or FNMR/FMR) reported in “developer’s performance test document” is equal or lower than the error rates specified in the FIA_MBV_EXT.1.2.

2.3.3.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS and AGD guidance

b. “Developer’s performance test document” meets all requirements in Section 7, “Developer’s performance test document and its assessment strategy” and valid rationale is provided by developer if “developer’s performance test document” doesn’t meet any requirements

c. FRR/FAR or FNMR/FMR measured by the developer’s performance testing is equal or lower than “defined value” specified in FIA_MBV_EXT.1.2

2.3.3.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

The evaluator shall also report a justification why evaluator determines the rationale provided by developer is valid if “developer’s performance test document” doesn’t meet any requirements in Section 7, “Developer’s performance test document and its assessment strategy”.

2.3.4. EA for FIA_MBV_EXT.2

2.3.4.1. Objective of the EA

Mobile biometric verification performance depends on quality of samples that is compared to templates. The evaluator shall examine that the TOE checks the quality of samples based on the assessment criteria to verify a user with an adequate reliability.

The evaluator shall keep in mind that the assessment criteria for different biometric modalities may not be the same. The evaluator shall evaluate each biometric modality separately if the ST author selects multiple biometric modalities in FIA_MBV_EXT.1.

The evaluator shall also keep in mind that assessment criteria used for templates and samples may not be the same. Assessment criteria for templates may be stricter than the one for samples.

2.3.4.2. Dependency

The evaluator shall perform the EAs for FIA_MBE_EXT.1, FIA_MBE_EXT.2 and FIA_MBV_EXT.1 first to confirm the mobile biometric enrolment and verification can be done correctly.

2.3.4.3. Tool types required to perform the EA

Developer shall provide a test platform for the evaluator to conduct the test described in the Assessment Strategy.

2.3.4.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBV_EXT.2 at high level description
b. AGD guidance shall provide clear instruction for a user to verify him/herself
c. Supplementary information (Assessment criteria for samples) shall describe assessment criteria for creating samples

AGD guidance may include online assistance, prompts or warning provided by the TOE during the verification attempt.

2.3.4.5. Assessment Strategy

2.3.4.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS to understand how the TOE checks quality of samples captured. The evaluator shall also examine the guidance, including online assistance or prompts provided by the TOE, about how the TOE supports a user to verify him/herself correctly and how the TOE behaves when low quality samples are presented to the TOE.

The evaluator shall examine that “assessment criteria for samples” to check that how the TOE checks the quality of samples based on its assessment criteria. The “assessment criteria for samples” may include;

a. Quality requirements for the biometric sample to ensure that a sufficient amount of distinctive features is available
b. Method to quantify the quality of samples (e.g. method to generate quality score)
c. Assessment criteria to accept the sample of sufficient utility (e.g. compare quality score to quality threshold)
d. Quality standard that the TOE uses to perform the assessment if the TOE follows such standard (e.g. NFIQ for fingerprint)

2.3.4.5.2. Strategy for ATE_IND

The evaluator shall perform the following test to verify that the TOE checks the quality of samples based on the assessment criteria.

The following test requires the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

a. Step 1: The evaluator shall present biometric samples of low quality for mobile biometric verification that don't satisfy the assessment criteria described in "assessment criteria for samples"
b. Step 2: The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that the TOE rejects any samples that don't meet the assessment criteria specified in the "assessment criteria for samples"

2.3.4.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS, AGD guidance and "assessment criteria for samples"
b. The TOE accepts only samples that pass the assessment criteria through the independent testing

2.3.4.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.3.5. EA for FIA_MBV_EXT.3

2.3.5.1. Objective of the EA

The evaluator shall verify that the TOE prevents use of artificial Presentation Attack Instruments (PAI). This section defines EAs derived from ASE_TSS.1, AGD_OPE.1 and ADV_FSP.

The main part of EA for FIA_MBV_EXT.3 is evaluator's testing using artificial PAI. The Section 6, "Evaluation Activities for FIA_MBV_EXT.3" defines EAs for ATE_IND.1 and AVA_VAN.1 in detail that the evaluator shall perform during the testing.

2.3.5.2. Dependency

The evaluator shall perform the EAs for FIA_MBE_EXT.1, FIA_MBE_EXT.2, FIA_MBV_EXT.1 and FIA_MBV_EXT.2 first to confirm the mobile biometric enrolment and verification can be done correctly.

2.3.5.3. Tool types required to perform the EA

No tool is required for this EA.

2.3.5.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBV_EXT.3 at high level description. TSS may only states that the TOE implements PAD mechanism and may not disclose any information about the PAD mechanism itself in detail because such information is beyond the scope of assurance level claimed by [BIOPP-Module] and may also be exploited by attackers

b. AGD guidance may provide information about how the TOE reacts when artificial PAI is detected

2.3.5.5. Assessment Strategy

2.3.5.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS and AGD guidance to check that the TSS or AGD guidance states that the TOE prevents the use of artificial PAI.

Main part of EA is evaluator's testing defined in Section 6, "Evaluation Activities for FIA_MBV_EXT.3". The evaluator should not require the detail design description of PAD from developer because it's beyond the scope of assurance level claimed in [BIOPP-Module].

2.3.5.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. TSS or AGD guidance states that the TOE prevents the use of artificial PAI

2.3.5.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.4. Protection of the TSF (FPT)

2.4.1. EA for FPT_BDP_EXT.1

2.4.1.1. Objective of the EA

[BIOPP-Module] assumes that the mobile device provides the Secure Execution Environment (SEE), an operating environment separate from the main mobile device operating system. Access to the SEE is highly restricted and may be made available through special processor modes, separate security processors or a combination to provide this separation.

Evaluation of this SEE is out of scope of [BIOPP-Module] and the evaluator doesn't need to evaluate this environment itself. However, the evaluator shall examine that the TOE processes any plaintext biometric data within the security boundary of the SEE. The SEE is responsible for preventing any entities outside the environment from accessing plaintext biometric data.

FPT_BDP_EXT.1 applies to plaintext biometric data being processed during mobile biometric enrolment and verification. Protection of transmitted and stored biometric data is out of scope of this EA and covered by FPT_BDP_EXT.2 and FPT_BDP_EXT.3 respectively.

2.4.1.2. Dependency

There is no dependency to other EAs defined in this SD.

2.4.1.3. Tool types required to perform the EA

No tool is required for this EA.

2.4.1.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FPT_BDP_EXT.1 at high level description

2.4.1.5. Assessment Strategy

2.4.1.5.1. Strategy for ASE_TSS

As depicted in Figure 1 of [BIOPP-Module], biometric characteristics is captured by biometric capture sensor and then sent to the processors in mobile device for signal processing, PAD and comparison and return the decision outcome. This is a typical process flow of mobile biometric verification; however, biometric capture sensor may do the all tasks within the sensor. In either case, all TSF modules (i.e. biometric capture sensor and any software running in biometric capture sensor and mobile device processors) that process plaintext biometric data must be separated from any entities outside the SEE. Any plaintext biometric data must not be accessible from any entities outside the SEE.

In any cases, the evaluator shall examine the TSS to confirm that;

a. All TSF modules run within the SEE and any entities outside the SEE including mobile device operating system can’t interfere with processing of these modules
    - If biometric capture sensor returns plaintext biometric data, any entities outside the SEE can’t access the sensor and data captured by the sensor
b. All plaintext biometric data is retained in volatile memory within the SEE and any entities outside the SEE including mobile device operating system can’t access these data. Any TSFIs doesn’t reveal plaintext biometric data to any entities outside the SEE

The evaluator shall keep in mind that the objective of this EA is not evaluating the SEE itself. This EA is derived from ASE_TSS.1.1 which requires that the TSS to provide potential consumers of the TOE with a high-level view of how the developer intends to satisfy each SFR. The evaluator shall check the TSS to seek for a logical explanation why above a) – c) is satisfied considering this scope of the requirement.

2.4.1.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. information necessary to perform this EA is described in the TSS

2.4.1.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.4.2. EA for FPT_BDP_EXT.2

2.4.2.1. Objective of the EA

The intention of this requirement is to prevent the logging, backing up or sending of plaintext biometric data to a service that transmits the information outside the security boundary of the SEE.

For example, the TOE may transmit plaintext biometric data to the developer's server for diagnostic purpose with a consent of the user. However, the TOE must not send plaintext biometric data as it is to the developer. The TOE must encrypt the data first before sending it.

In any case, the evaluator shall determine that the TOE doesn't transmit any plaintext biometric data outside the security boundary of the SEE.

2.4.2.2. Dependency

The evaluator shall perform the EAs for FPT_BDP_EXT.1 first to confirm the TSF processes any plaintext biometric data within the security boundary of the secure execution environment.

2.4.2.3. Tool types required to perform the EA

No tool is required for this EA.

2.4.2.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FPT_BDP_EXT.2 at high level description
b. AGD guidance shall describe all functions that transmit biometric data

2.4.2.5. Assessment Strategy

2.4.2.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS and AGD guidance to identify any functions that transmit biometric data to any entities outside the SEE and type of biometric data that is transmitted.

If the TOE transmits biometric data, the evaluator shall examine that the activities that happen on the data transmission to confirm that;

a. The TOE requires an explicit user consent and user authentication to enable the transmission
b. The TOE never transmits plaintext biometric data to outside the SEE. This means;
   1. The TOE encrypts plaintext biometric data to be transmitted using the cryptographic functions evaluated based on [MDFPP] within the SEE
   2. If the TOE stores the encrypted biometric data outside the SEE for transmission, the TOE

deletes such data after the transmission

3. If the TOE displays the plaintext biometric data to the user to seek approval for transmission, such process is performed within the SEE

c. The TOE disables the transmission right after the TOE achieves its purpose

2.4.2.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. information necessary to perform this EA is described in the TSS and AGD guidance

2.4.2.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.4.3. EA for FPT_BDP_EXT.3

2.4.3.1. Objective of the EA

Plaintext biometric data, especially templates, are highly sensitive personal data because biometric characteristics may be recovered from them. Plain text biometric data shall be processed within the SEE as required by FPT_BDP_EXT.1. However, part of plaintext biometric data including templates may need to be stored in mobile device for mobile biometric verification. However, protection of such stored biometric data is not covered by FPT_BDP_EXT.1.

The evaluator shall confirm that the TOE encrypts plaintext biometric data within the SEE before storing it in any non-volatile memory that entities outside the SEE can get access to. If the evaluator confirms that the TOE doesn’t store plaintext biometric data outside the SEE (e.g. biometric capture sensor processes biometric data within the sensor and return only decision outcome to the TSF modules running inside the SEE) during performing the EA of FPT_BDP_EXT.1, this requirement deems satisfied.

2.4.3.2. Dependency

The evaluator shall perform the EAs for FPT_BDP_EXT.1 first to confirm the TSF processes any plaintext biometric data within the security boundary of the secure execution environment.

2.4.3.3. Tool types required to perform the EA

Developer shall provide a test platform for the evaluator to conduct the test described in the Assessment Strategy.

2.4.3.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FPT_BDP_EXT.3 at high level description

b. Supplementary information (file list/format and cryptographic algorithm) shall list locations and format of files that contain biometric data, and cryptographic algorithm used to encrypt those files

2.4.3.5. Assessment Strategy

2.4.3.5.1. Strategy for ASE_TSS

The evaluator shall examine the TSS to understand the activities that happen on mobile biometric enrolment and verification relating to encrypting and storing biometric data. The evaluator shall confirm that;

a. The TSS lists type of biometric data that the TOE stores in non-volatile memory outside the SEE
b. The TOE encrypts all plaintext biometric data listed in the TSS within the SEE before storing it in the non-volatile memory
c. The TOE uses cryptographic functions evaluated based on [MDFPP] to encrypt the data

2.4.3.5.2. Strategy for ATE_IND

The evaluator shall perform the following test to verify that the TOE encrypts plaintext biometric data if the TOE stores the data in non-volatile memory outside the SEE.

The following test requires the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

a. Step 1: The evaluator shall check that all cryptographic algorithms listed in “file list/format and cryptographic algorithm” are successfully evaluated based on [MDFPP]
b. Step 2: The evaluator shall load an app onto the mobile device. This app shall attempt to traverse over all file systems and report any newly created files
c. Step 3: The evaluator shall perform mobile biometric enrolment and verification and run the app to list new files
d. Step 4: The evaluator shall compare files reported by the app and ones listed in “file list/format and cryptographic algorithm”
e. Step 5: If evaluator finds newly created files not listed in “file list/format and cryptographic algorithm”, the evaluator shall confirm that those files don’t include plaintext biometric data with the support from developer
f. Step 6: For all files listed in “file list/format and cryptographic algorithm”, the evaluator shall display the contents of files and check that the files are encrypted. The evaluator can assume that encryption is done correctly because the TOE uses cryptographic algorithms evaluated based on [MDFPP]. The evaluator shall compare the content of files to the format defined in “file list/format and cryptographic algorithm” to check that the files don’t follow the defined format to implicitly assume files are encrypted.

2.4.3.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS.

b. The TOE encrypts any plaintext biometric data before storing it outside the SEE through the independent testing

2.4.3.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

2.4.4. EA for FPT_PBT_EXT.1

2.4.4.1. Objective of the EA

Only authenticated user can add his/her own templates during mobile biometric enrolment as defined in the FIA_MBE_EXT.1 and those templates are not stored outside the SEE without encryption as required by the FPT_BDP_EXT.3. However, the TOE may provide functions (e.g. revocation of templates) to access the templates. The evaluator shall confirm that only authenticated user either using a PIN, password or by other secure means, as specified by the ST author can access the templates through the TSFI provided by the TOE.

2.4.4.2. Dependency

The evaluator shall perform the EA for FIA_MBE_EXT.1 first to confirm the mobile biometric enrolment can be done correctly.

2.4.4.3. Tool types required to perform the EA

No tool is required for this EA.

2.4.4.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FPT_BDP_EXT.1 at high level description

b. AGD guidance shall describe how the user can access the templates

2.4.4.5. Assessment Strategy

2.4.4.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS and AGD guidance to identify any TSFI through which the user can access (e.g. revoke) the templates. The evaluator shall confirm that those TSFI requires either using a PIN, password or by other secure means, as specified by the ST author.

2.4.4.5.2. Strategy for ATE_IND

The evaluator shall perform the following test to verify that the TOE protects the templates as specified in TSS and AGD guidance.

a. Step 1: The evaluator shall perform functions through the TSFIs that access the templates

b. Step 2: The evaluator shall check that the TSFI requires either using a PIN, password or by other secure means, as specified by the ST author.

2.4.4.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS and AGD guidance
b. The TOE protects the templates either using a PIN, password or by other secure means, as specified by the ST author

2.4.4.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

3. Evaluation Activities for Selection-Based Requirements

3.1. Identification and Authentication (FIA)

3.1.1. EA for FIA_HYB_EXT.1

3.1.1.1. Objective of the EA

A hybrid authentication mechanism is one where a user has to submit a combination of biometric sample and PIN or password with both to pass and without the user being made aware of which factor failed, if either fails. The evaluator shall verify that the TOE use only selected modality for this hybrid authentication.

3.1.1.2. Dependency

The evaluator shall perform the EA for FIA_MBE_EXT.1 first to confirm the mobile biometric enrolment can be done correctly.

3.1.1.3. Tool types required to perform the EA

No tool is required for this EA.

3.1.1.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBE_EXT.1 at high level description
b. AGD guidance shall describe how the hybrid authentication can be done

3.1.1.5. Assessment Strategy

3.1.1.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS to understand how the TOE verify a user with his/her biometric characteristics and PIN or password. The evaluator shall also examine the AGD guidance about how the TOE supports a user to verify him/herself correctly and how the TOE behaves when hybrid authentication is succeeded or failed.

3.1.1.5.2. Strategy for ATE_IND

The evaluator shall perform the following test to verify that the TOE protects the templates as specified in TSS and AGD guidance.

a. Step 1: The evaluator shall configure and perform hybrid authentication

b. Step 2: The evaluator shall check that the TOE can conduct hybrid authentication as specified, especially, when either factor is failed, the TOE doesn't reveal any information about which factor is failed

3.1.1.6. Pass/Fail criteria

The evaluator can pass this EA only if the evaluator confirms that:

a. Information necessary to perform this EA is described in the TSS and AGD guidance

b. The TOE can conduct hybrid authentication using modality as specified by the ST author

3.1.1.7. Requirements for reporting

The evaluator shall report the summary of result of EA defined above, especially how the evaluator reaches the Pass/Fail judgement based on the Pass/Fail criteria.

4. Evaluation Activities for Optional Requirements

4.1. Identification and Authentication (FIA)

4.1.1. EA for FIA_MBE_EXT.3

The evaluator shall refer the EA for FIA_MBV_EXT.3 to perform evaluation of this SFR.

4.2. User data protection (FDP)

4.2.1. EA for FDP_RIP.2

The evaluator shall refer the EA for FCS_CKM_EXT.4 in [MDFPP] to perform evaluation of this SFR.

5. Evaluation Activities for SARs

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

5.1. Class ASE: Security Target

[MDFPP] doesn't define any EAs and there is no additional EAs for [BIOPP-Module].

5.2. Class ADV: Development

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

5.3. Class AGD: Guidance Documentation

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

5.3.1. 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 [MDFPP] and the operational guidance doesn't 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 for FIA_MBV_EXT.3". The evaluator shall also follow this note depending on the result of the penetration testing for PAD.

5.3.2. 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].

5.4. Class ALC: Life-cycle Support

The evaluator shall take the following additional application notes into account to perform EAs defined in [MDFPP] for [BIOPP-Module]. There is no application note for EA for ALC_CMS.1 and ALC_TSU_EXT.

5.4.1. Application note for EA of ALC_CMC.1

[BIOPP-Module] is intended to be used with [MDFPP] 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.

5.5. Class ATE: Tests

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

5.5.1. Application note for EA of ATE_IND.1

Same EA should be applied to [BIOPP-Module] except SFR FIA_MBV_EXT.3 (**Presentation attack detection for mobile biometric verification**). The evaluator shall perform EAs defined in Section 6, “Evaluation Activities for FIA_MBV_EXT.3” for FIA_MBV_EXT.3.

5.6. Class AVA: Vulnerability Assessment

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

5.6.1. Application note for EA of AVA_VAN.1

Same EA should be applied to [BIOPP-Module] except SFR FIA_MBV_EXT.3 (**Presentation attack detection for mobile biometric verification**). The evaluator shall perform EAs defined in Section 6, “Evaluation Activities for FIA_MBV_EXT.3” for FIA_MBV_EXT.3.

6. Evaluation Activities for FIA_MBV_EXT.3

6.1. Introduction

The evaluator shall perform the following two types of EAs or testing to evaluate the FIA_MBV_EXT.3 (**Presentation attack detection for mobile biometric verification**).

a. EAs for ATE_IND.1 (Independent testing - conformance)

b. EAs for AVA_VAN.1 (Vulnerability survey)

ATE_IND.1 requires the evaluator to demonstrate that the TOE operates in accordance with its design representations described in TSS or AGD guidance (As described in [MDFPP], a formal or complete specification of PAD interface is not required but the evaluator should examine interface information presented in the TSS and AGD guidance).

However, [BIOPP-Module] doesn’t require such design representations about PAD (e.g. how the TOE checks the liveness of the object) in TSS or AGD because those information is beyond the scope of assurance level claimed by [BIOPP-Module]. Therefore, this SD doesn’t also require the evaluator to test the functional aspects of PAD based on those design representations.

Instead, this SD requires the evaluator to conduct ATE_IND.1 evaluation (i.e. independent testing) in black-box manner. However, difficulty of black-box testing for PAD, as described in [ISO30107-3], is that it's very difficult to have a comprehensive model of all possible PAIs. Therefore, it may be possible that different evaluator could use a different set of PAIs and see different test results for the same TOE.

To solve this issue, the Biometric Security iTC (BIO-iTC) creates [Toolbox]. This [Toolbox] defines the common PAIs for PAD testing based on publicly available information (e.g. research papers), experiences and knowledge shared among the BIO-iTC members.

[Toolbox] includes a collection of test items for each biometric modality. Each test item describes the procedure to create PAIs and the method to present them to the TOE in sufficient detail to enable the test to be repeatable.

The same [Toolbox] can also be used for AVA_VAN.1 evaluation (i.e. penetration testing) because AVA_VAN.1 requires the evaluator to devise tests based on information available in the public domain. However, [Toolbox] should be used in a different manner for AVA_VAN.1 evaluation. The following section explains how [Toolbox] should be used in EAs for ATE_IND.1 and AVA_VAN.1.

6.2. EAs for ATE_IND.1 (Independent testing - conformance)

6.2.1. Independent test activities using [Toolbox]

As described in previous section, [Toolbox] defines test items to create a representative set of PAIs that the evaluator shall use for the testing. During ATE_IND.1 evaluation, the evaluator shall conduct all test items in [Toolbox] for the selected modalities without any change. The evaluator is not allowed to skip any test items in the [Toolbox] to maintain compatibility between different evaluations.

During the independent testing, the evaluator may find PAIs that are incorrectly matched to the enrolled target user however, the evaluator may not be able to reliably reproduce a successful presentation attack.

[Toolbox] defines the Pass/Fail criteria, maximum attack presentation match rate for PAIs. The evaluator shall follow the [Toolbox] criteria for the number of PAI presentations and confirm that the TOE's match rate is below the specified criteria during the independent testing. The evaluator shall assign fail verdict to those TOE that doesn't satisfy the criteria.

The PAIs that pass the criteria but show the higher attack presentation match rate will be tested again during the AVA_VAN.1 evaluation.

[Toolbox] does not necessarily cover all biometric modalities. If the developer wants to evaluate modalities not currently included in [Toolbox], the developer and evaluator shall contact to the BIO-iTC to work together to extend [Toolbox]. Upon the BIO-iTC approval of this extension, the evaluator can proceed with PAD evaluation for new modality.

6.2.2. Justification for EAs for ATE_IND.1

The EAs presented in this section are derived from ATE_IND.1-3, ATE_IND.1-4 and ATE_IND.1-7 and their verdicts will be associated with those work units.

[Toolbox] describes a test subset and test documentation that is sufficiently detailed to enable the tests to be reproducible (ATE_IND.1-3 and ATE_IND.1-4). [Toolbox] also defines Pass/Fail criteria that support evaluator's decision (ATE_IND.1-7).

6.3. EA for AVA_VAN.1 (Vulnerability survey)

6.3.1. Penetration test activities using [Toolbox]

This Section describes EAs for AVA_VAN.1 step by step following the order of AVA_VAN.1 CEM work units.

6.3.1.1. Search for new PAIs

The evaluator shall search publicly available information that is published after the publication date of [Toolbox] to look for new PAI species. New PAI species are those PAIs that are out of scope of [Toolbox] and need to be made in the completely different way with the significantly different materials that are not covered by [Toolbox].

Those new PAI species that can be made by slightly modifying test items in [Toolbox] are covered by Section 6.3.1.3.1, "No new PAIs found test plan".

6.3.1.2. Identify candidate PAIs for testing

The evaluator shall perform EAs in Section 6.3.1.2.1, "No new PAIs found" if there is no new PAI species found at the previous step. Otherwise, follow Section 6.3.1.2.2, "New PAIs found".

6.3.1.2.1. No new PAIs found

If the evaluator can't find such new PAI species, the evaluator doesn't need to devise new test items in addition to those defined in [Toolbox] because the BIO-iTC develops test items based on all publicly available information published by the publication date of [Toolbox]. The BIO-iTC also verifies that test items cover all existing PAI species that are within the scope of Basic attack potential defined in Section 9, "Attack Potential and TOE resistance". Therefore, the evaluator doesn't need to repeat this process.

6.3.1.2.2. New PAIs found

If the evaluator can find new PAI species, the evaluator shall consider the following factors to examine whether those new PAI species can be used in the actual operational environment or not.

a. Attacker's motivation

   For enhanced security that is easy to use, the TOE implements mobile biometric verification on a device once it has been "unlocked". The initial unlock is generally done by a PIN/password which is required at startup (or possibly after some period of time), and after that the user is able to use a registered biometric characteristic to unlock access to the mobile device. The SD assumes that the mobile biometric verification is being used in accordance with USE CASE 1: Mobile biometric verification for unlocking the mobile device.

Attacker may use any tools or materials that are normally available at home and normal office environment such as laptop PC or office printer to attack the TOE. Attacker may also use any services (e.g. printing services to print a high-resolution photo of target users to create a face PAI) if such services are available at low cost.

1. Assumptions in [BIOPP-Module]

   [BIOPP-Module] defines **A.User** and evaluator shall assume that the mobile devices are configured securely by users. Especially evaluator shall make the following assumptions:

   1. A user enrol him/herself following guidance provided by the TOE
   2. Mobile device is securely configured, and maximum number of unsuccessful biometric authentication attempts is limited

      For efficiency, the evaluator can increase the maximum number of unsuccessful biometric authentication attempts to conduct the testing. However, as the mobile device shall be evaluated in the evaluated configuration, any attack needs to succeed within the allowed number of biometric authentication attempts defined in the ST to be considered a successful attack.

      [BIOPP-Module] also defines **A.Protection** and evaluator shall assume that biometric data is adequately protected. Especially evaluator shall make the following assumptions:

   3. Attacker can’t access to the result of PAD subsystem, so they can’t tune the PAIs based on the PAD score
   4. Attacker can’t gain the templates from the mobile device to create the PAIs

c. Attack potential

   The evaluator is not expected to determine the exploitability for new PAI species beyond those for which a Basic attack potential is required to create and present. Therefore, the evaluator shall determine that attack potential required to use new PAI species is within the scope of the Basic attack potential referring Section 9, “Attack Potential and TOE resistance”.

6.3.1.3. Produce test plan

The evaluator shall perform EAs in Section 6.3.1.3.1, “No new PAIs found test plan” if there is no new PAI species found in previous step. Otherwise, follow Section 6.3.1.3.2, “New PAIs found test plan”.

6.3.1.3.1. No new PAIs found test plan

The evaluator shall select those PAIs that show higher attack presentation match rate at the independent testing. The evaluator shall test them extensively during the penetration testing.

If there is no such PAIs, the evaluator should select “higher quality” PAIs. “Higher quality” means that PAIs are closer in resemblance to the biometric characteristics of the target user (e.g. higher resolution photo for face PAI).

The evaluator may recreate the PAIs selected for penetration testing to improve their quality taking following approaches.

a. Modify the creation process of PAIs

   The evaluator may modify the process in [Toolbox] to improve the PAIs.

   For example, in case of finger or palm vein verification, the evaluator needs to capture the vein pattern from a target user using a NIR-camera and print it out to create the PAI (i.e. printed vein pattern). However, quality of the vein pattern may vary depending on configuration of tools (e.g. intensity of NIR light for NIR-camera) or type of materials (e.g. type of paper).

   During the penetration testing, the evaluator may change those various factors to recreate PAIs with clearer vein pattern for the penetration testing.

   However, the evaluator shall recreate the PAI at the similar cost and time as required for the original PAI to stay within the Basic attack potential.

b. Change test subjects

   The evaluator may follow the same procedure in [Toolbox] to recreate PAIs, however, from different test subjects from ones used for the independent testing.

   For example, in case of finger or palm vein verification, men normally have thicker blood vessel than women. So, the evaluator may change the test subject who has thicker blood vessel to capture the clearer vein pattern.

The evaluator may also increase time for PAI presentation training and habituation to find the better presentation method.

For example, in case of finger or palm vein verification, quality of vein pattern gained from the sensor (NIR-camera) of the TOE may vary depending on the distance between the PAI and sensor, and how to present the PAI to the TOE. However, it’s not possible for the evaluator to know the best distance or presentation method for the PAI in advance because this SD requires the evaluator to test the TOE in black-box manner. The evaluator may simply increase the number of attempts to find the best distance or presentation through trial and error process.

6.3.1.3.2. New PAIs found test plan

If the evaluator can find the new PAI species that can be used for the penetration testing, the evaluator shall produce the test item for those new PAI species and add them to [Toolbox]. The evaluator shall create those new test items at the same format and level of detail as existing ones in [Toolbox].

The evaluator shall also inform the BIO-iTC for this update because the BIO-iTC is responsible for maintaining [Toolbox].

The evaluator shall also perform EAs in Section 6.3.1.3.1, “No new PAIs found test plan” to produce the test plan based on the result of independent testing.

6.3.1.4. Conduct the penetration testing

The evaluator shall conduct the penetration testing based on the test plan created in the previous step.

The evaluator shall select those PAIs that may succeed the attack at higher probability as described in Section 6.3.1.3, “Produce test plan” for the penetration testing.

However, the evaluator shall not spend more than one week for independent and penetration testing, considering the assurance level claimed by [BIOPP-Module].

6.3.1.5. Determine Pass/Fail of penetration testing

The evaluator shall determine that the TOE, in its operational environment, is resistant to an attacker possessing a Basic attack potential. The evaluator shall make this determination based on guidance provided in Section 9.3, “Pass/Fail criteria for EAs for FIA_MBV_EXT.3”.

6.3.2. Justification for EAs for AVA_VAN.1

The EAs presented in this section are derived from AVA_VAN.1-3, AVA_VAN.1-4, AVA_VAN.1-5, AVA_VAN.1-6, AVA_VAN.1-7 and AVA_VAN.1-10 and their verdicts will be associated with those work units.

EAs in the Section 6.3.1.1, “Search for new PAIs” and Section 6.3.1.2, “Identify candidate PAIs for testing” complements evaluator’s action for searching publicly available information and identifying potential vulnerabilities (e.g. new PAI) (AVA_VAN.1-3, AVA_VAN.1-4 and AVA_VAN.1-5).

EAs in Section 6.3.1.3, “Produce test plan” and Section 6.3.1.4, “Conduct the penetration testing” complements evaluator’s action for creating the test plan and conducting the penetration testing for PAD (AVA_VAN.1-6 and AVA_VAN.1-7)

EAs in Section 6.3.1.5, “Determine Pass/Fail of penetration testing” provides specific guidance for pass or failure of the testing (AVA_VAN.1-10).

7. Developer’s performance test document and its assessment strategy

This Section describes requirements for the developer’s performance test document (hereafter “test document”) and its assessment strategy.

The developer shall create the test document to report the result of performance testing (e.g. FRR/FAR or FNMR/FMR).

The evaluator shall examine the test document following the Assessment Strategy defined in Section 2.3.3, “EA for FIA_MBV_EXT.1” to verify that the developer’s performance test was done in an objective and repeatable manner to check the trustworthiness of the measured error rates.

The requirements defined in this Section are created based on [ISO19795-1] and [ISO19795-2].

7.1. Requirements for the test document

The developer shall provide the test document for CC evaluations that claim a conform to [BIOPP-Module]. This Section defines required content of the test document that is inputted to the EA for FIA_MBV_EXT.1.

7.2. Summary of contents

Table 1 shows items that shall be reported in the test document. Name or structure of test document doesn’t need to follow Table 1. However, all items in Table 1 shall be written somewhere in the test document. Also, if some items are not included in the test document, the developer shall provide a rationale for such exclusion to the evaluator.

Table 2. Reporting items

Section	Item
TD.1	Overview of the performance testing
TD.2	Target application and influential factors
TD.3	Test subject selection
TD.4	Test instructions and training
TD.5	Test subject management
TD.6	Test procedure

7.3. Reporting items description

This Section describes each item in Table 1 in detail. All items are created based on [ISO19795-1] and [ISO19795-2] however some of them are modified to adjust to the CC evaluation.

7.3.1. TD.1 Overview of the performance testing

The developer shall report following general information about the performance testing.

a. Performance test configuration

   The test document shall report the following information to uniquely identify the test configuration of the performance testing. Information stated here shall be consistent with the ST.

   1. TOE reference

      Information that uniquely identifes the TOE shall be reported. [BIOPP-Module] is intended to be used with [MDFPP] and reference for the mobile device can be used as the TOE reference only if the reference for the mobile device also uniquely identifies the biometric system embedded in the mobile device

    Modification to the TOE for performance testing, if any, shall be reported (e.g. The TOE is modified to export biometric data for off-line testing). The rationale that such modification doesn’t affect the TOE performance shall also be provided. For example, the developer may claim that the performance is not affected because modified code isn’t executed during mobile biometric verification or the developer may run regression test to verify that modification doesn’t change the result of verification (e.g. similarity score).

2. TOE configuration

    Any configurable parameters or setting of the TOE that may affect the performance shall be reported. Value of each parameter set for the testing shall also be provided. For example, if threshold (e.g. decision threshold and image quality threshold) is configurable by users, value of threshold set for the testing shall be reported.

3. Performance test tools

    Information that uniquely identify all testing tools (e.g. SDK) used for the performance testing shall be reported.

b. Result of the performance testing

The test document shall report the following items to provide the result of testing.

1. Test period and location

    Timeline for the performance testing (samples or templates may be collected over multiple sessions) and location of testing shall be reported.

2. Modality used for mobile biometric verification

    The performance testing shall be done for all modalities selected in FIA_MBV_EXT.1. Result of testing for each modality shall be reported separately.

3. Definition of genuine and imposter transaction

    If FAR/FRR is selected in FIA_MBV_EXT.1, the test document shall clearly define what constitutes the transaction based on the guidance provided in transaction and samples and the same rule shall be applied consistently throughout the performance testing.

4. Number of test subjects, templates and samples

    The following numbers used for calculating FMR/FNMR or FAR/FRR shall be reported. See transaction and samples for requirements for number of test subjects, enrolment templates and samples.

    This Section assumes that at least the FMR or FAR is measured through offline testing (i.e. cross-comparison) to achieve the maximum number of attempts or transactions. FNMR or FRR may be measured through online or offline testing.

    - Test subjects

Number of test subjects who participated in the testing shall be reported.

- Enrolment templates

  Number of enrolment templates used for testing shall be reported.

  Note all test subjects may generate the templates successfully and total number of templates may be less than (number of test subjects) × (number of body parts of a test subject).

- Samples

  Number of samples collected for each body part and total number of samples collected from all test subjects shall be reported.

  Not all test subjects may generate the samples successfully and total number of samples may be less than (number of test subjects) × (number of body parts of a test subject) × (number of samples collected for each body part).

5. Result of testing

   Error rates measured by the performance testing shall be reported.

   If FAR and FRR is selected in FIA_MBV_EXT.1, number of genuine and imposter transaction shall also be reported.

   If FMR and FNMR is selected in FIA_MBV_EXT.1, number of genuine and imposter attempts shall also be reported.

7.3.2. TD.2 Target application and influential factors

Test document shall specify a target application modelled in the test, such as mobile biometric verification in an indoor office environment with a habituated crew.

Test document shall also report influential factors that may influence performance, measures to control such factors and under what factors the performance testing was conducted.

Influential factors can be determined by referring appropriate documents (e.g. [ISO19795-3]) or referring the product datasheet (e.g. operating temperature). These factors should be consistent with the target application.

The following factors are examples of controlling factors for finger/hand vein verification. The developer shall define these factors properly, for example, based on [ISO19795-3]. Any information that are useful in the context of the used biometric modality shall be considered by the developer to determine the factors.

It’s recommended to control all influential factors appropriately because different error rates may be measured under different influential factors.

a. Test subject demographics

1. Age: age distribution ratio by arbitrary age groups (e.g., 1, 5, 10 years)
2. Gender: male/female distribution
3. Ethnic origin: Distribution ratio by ethnic origin. Category of ethnic origin can be arbitrarily defined by developer

b. Posture and positioning

Posture of test subject or positioning of his/her hand/finger (e.g. Orientation of hand/finger in relation to the sensor or distance to the sensor). Such information should be consistent with the TOE operational guidance or automated feedback provided by the TOE.

c. Indoor or outdoor

Indoor or outdoor environment in which testing is to be conducted. In case of outdoor environment, other factors affecting the performance (e.g. environmental illumination) should also be reported.

d. Temperature

Range of temperature at which the testing is to be conducted (e.g. “Testing was conducted in an air-conditioned environment where temperature was kept between X and Y degrees”).

e. Time interval

Time interval (e.g. minimum, maximum and average time) between enrolment and verification.

f. Habituation

The degree to which the test subject is familiarized with the TOE (e.g. frequency of use of the TOE)

g. Template adaptation

How much template adaptation may occur prior to measuring the FMR/FAR and FNMR/FRR if the TOE is able to adapt the templates over time with the aim to reduce the error rates

7.3.3. TD.3 Test subject selection

Selection method of test subjects shall be reported (e.g. gather test subjects from developer’s employees or recruit them from public). It is recommended that demographics of test subjects follow the target application.

7.3.4. TD.4 Test instructions and training

Instructions and training given to the test subjects shall be reported. The same instructions and training shall be given to the all test subjects.

a. Test information and general test instructions

Test information and general test instructions given to test subject prior or after biometric data collection shall be reported. Such instructions shall be consistent to automated guidance or feedback given by the TOE or instructions described in the TOE operational guidance. Testing shall not be adjusted to the TOE specification that is not described in the TOE operational guidance

b. Confirmation of habituation

   Method for how to confirm the level of subject habituation prior to biometric data collection shall be reported. If the habituation was confirmed through training, method to ensure the consistency of training among test subjects and the tools used for training shall be reported (e.g. developer can prepare the script for training in advance and apply it to all test subjects to ensure the consistency)

7.3.5. TD.5 Test subject management

The following information about test subject management shall be reported. Proper management is necessary to avoid human errors that may occur during the testing.

a. Management processes

   Biometric data can be corrupted by human error during the collection process (e.g. using a middle finger when the index finger is required). The test subject management processes to avoid such errors shall be reported. Management processes shall cover the following processes

   1. Method of initial test subject registration
   2. Method of ensuring test subject uniqueness
   3. Method of avoiding data collection errors (e.g. Use of data collection software minimizing the amount of data requiring keyboard entry)

7.3.6. TD.6 Test procedure

A test protocol for the testing shall be reported. The following items shall be covered.

a. Type of attempt or transaction

   Whether the attempt or transaction is executed online or offline shall be reported. Online means that enrolment and verification is executed at the time of image submission. Offline means that enrolment and verification is executed separately from image submission.

b. Test flow

   Details of flow of genuine and imposter attempt or transaction to measure the error rates shall be reported. The same flow shall be applied to all test subjects.

   The developer shall maintain a log file in which each interaction with the TOE is recorded. The log shall include all test attempts, preparative or practice attempts, set-up procedure (e.g. setting a threshold) and maintenance activities (e.g. cleaning a sensor). Such a log file can be very useful to make sure the testing was conducted following the test flow.

c. Sample exclusion criteria

   Criteria for sample exclusion shall be reported. Test operator shall not manually discard nor use an automated mechanism to discard collected samples unless the samples conform to documented exclusion criteria. The number of excluded samples shall be reported. If transactions are failed because of such excluded samples, number of such failed transactions shall also be reported. These failed transactions shall be counted as failed transactions to calculate the error rates.

d. Advice or remedial action

   Advice or remedial actions to test subjects who fail to complete transactions or sample collections shall be reported. Such advice or remedial actions shall be limited to the minimum amount necessary because [BIOPP-Module] assumes that the mobile device is used by the single user without any support. The same advice or remedial actions shall be given to test subject at the same condition.

8. Requirement for the number of test subject, transaction and samples

The developer shall follow recommendations or minimum requirements below to conduct the performance testing to measure FAR/FMR and FRR/FNMR. The developer may exclude, modify or add some recommendations however, the developer shall show a clear rationale why such modifications could produce more accurate estimate of the performance.

8.1. Recommendations

8.1.1. Test scenario for mobile biometric verification

The developer shall follow the guidance in this Section to define the transaction if the developer selects FAR and FRR in FIA_MBV_EXT.1 or to define the number of samples per each test subject if the developer selects FMR and FNMR in FIA_MBV_EXT.1.

The user may use the mobile biometric verification in a different way.

Suppose the mobile device provides both Password Authentication Factor and BAF and user can use either of factor to unlock the device. One user may try to unlock the device with BAF until allowable maximum number of unsuccessful authentication attempts is exceeded. Another user may try to unlock the device with BAF only three times and switch to the password if all three attempts were failed.

It may also be possible for user to enrol multiple body parts (e.g. index and thumb fingerprint) or single body part for mobile biometric verification.

However, it’s not possible to evaluate all these scenarios to measure the performance but the developer shall refer the ST that claims conformance to [MDFPP] to define the scenario.

For example, if the ST sets the maximum number of unsuccessful authentication attempts for mobile fingerprint verification to five, the developer shall assume that the attacker makes all five fingerprint unlock attempts in succession to try to unlock the mobile device.

This means that if FAR and FRR are selected, the developer shall define that the genuine and imposter transaction is consisted up to five unlock attempts and only one transaction can be run by each user.

If FMR and FNMR are selected, the developer may follow the same scenario and collect five samples from each test subject. However, FMR/FNMR is a comparison subsystem measure while FAR/FRR is a system level measure, therefore FAR/FRR should be selected in the ST if the developer considers the specific test scenario to measure the performance.

The developer shall also select the most common scenario among users to conduct the performance testing. For example, if the user can enrol multiple fingerprints, the developer should assume that the user enrols index and thumb fingerprint if such enrolment is most common. FAR may increase and FRR may decrease if the user enrols multiple fingerprints however, performance of widely used configuration should be measured.

8.1.2. Maximum number of templates

Only one template can be generated from each body part (e.g. right index fingerprint, left hand vein or face) of test subject and used for the performance testing.

Quality of template may have significant impact on the mobile biometric verification performance. This SD assumes that the user is familiar with the mobile devices operation and enrol him/herself correctly following the AGD guidance provided by the developer. The test subject may make enough number of practice attempts to get familiar with the device operation before the final enrolment transaction.

8.1.3. Maximum number of samples per test subject

The developer shall define the maximum number of samples per test subject to be collected following the guidance provided in Section 8.1.1, “Test scenario for mobile biometric verification”.

8.1.4. Maximum number of transactions per test subject

Only one transaction can be run by each test subject because the mobile device locks the mobile biometric verification as required by [MDFPP] after the certain number of attempts are failed.

8.1.5. Statistical certainty for FAR/FMR

FMR/FAR shall be estimated following rule of 3 or 30 because these errors are most relevant to the security of the TOE and the trustworthiness of those values shall be evaluated statistically. While the rule of 3 would require that one test subject is only involved in one impostor transaction, it is commonly agreed that the statistical loss of computing all possible cross-comparisons between test subjects is acceptable. This SD allows full cross-comparison to estimate FAR/FMR.

This SD also allows cross-comparison of attempts/templates for ordered pair if there is no explicit reason that this cross-comparison hinders the accuracy of the result of performance testing. Cross-comparison of attempts/templates for ordered pair allows to compare between user A's template and user B's sample and user A's sample and user B's template separately. However, if the TOE's verification algorithm is symmetric and make no distinction between the ordered pair, this assumption can't be used.

This SD doesn't allow intra-individual comparison that is a comparison between one body part and another body part of the same test subject (e.g. comparison between right and left iris of the same user).

8.1.6. Statistical certainty for FRR/FNMR

Rule of 3 requires no error occurred for all attempts/transactions and rule of 30 may require too many attempts/transactions if the FNMR/FRR is quite low. Therefore, the developer may calculate FNMR/FRR directly from the result of performance testing without considering the statistical confidence.

8.2. Example – fingerprint verification

The developer defines that mobile fingerprint verification is consisted of 5 attempts using both right index and thumb fingerprint to unlock the mobile device and specify 0.01 % FAR and 1% FRR in FIA_MBV_EXT.1.

As described in the previous Section, the genuine and imposter transaction is consisted up to five unlock attempts using either of finger against each template for index and thumb finger and only one transaction can be run by each user.

In this scenario, at least 30,000 imposter transactions shall be conducted with no error to achieve this performance goal if the rule of 3 is applied. To run more than 30,000 imposter transactions, at least 174 test subjects shall be gathered (173 * 174 = 30,102) if cross-comparison for ordered pair is allowed. If number of test subjects is 174, only 1 genuine transaction can be failed to achieve 1% FRR (2/174 = 0.011 > 1%).

If the developer specifies 0.01 % FMR and 1% FNMR in FIA_MBV_EXT.1, at least 30,000 imposter attempts shall be made with no errors. To run more than 30,000 imposter attempts, at least 78 test subjects shall be gathered (77 * 78 * 5 = 30030) if cross-comparison for ordered pair is allowed. If number of test subjects is 78, the total number of genuine attempts is 78 * 5 = 390 and 3 genuine attempts can be failed to achieve 1% FNMR (4/390 = 0.0102 > 1%).

9. Attack Potential and TOE resistance

9.1. Calculating attack potential for generic biometric system

Attack potential is a function of expertise, resources and motivation, as is written in [CEM]. [CEM] provides general guidance for calculating attack potential for all type of IT products and doesn't take any specific characteristics of biometrics into account.

This section introduces a method for calculating attack potential for generic biometric systems.

9.1.1. Identification and exploitation of attacks

9.1.1.1. Identification of attacks

Identification corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary test equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. One of the outputs from identification could be a script that gives a step-by-step description of how to carry out the attack. This script is assumed to be used in the exploitation phase.

9.1.1.2. Exploitation of attacks

Exploitation corresponds to achieving the attack on an instance of the TOE in its exploitation environment using the analysis and techniques defined in the identification phase. It could be assumed that a different attacker carries out the exploitation, the technique (and relevant background information) could be available for the exploitation in the form of a script or set of instructions defined during the identification phase. This type of script is assumed to identify the necessary equipment and, for example, mathematical techniques used in the analysis, or presentation attack methods. Furthermore, this same information may also reduce the exploitation requirement to one of time measurement, whereas the identification phase may have required reverse engineering of hardware or software information hence the expertise requirement may be reduced.

NOTE For the evaluator, the work of the identification phase has to be fully performed: developing hardware and software, creating PAIs if any, etc. The rating of this phase corresponds to the "real spending" in defining the attack. For the exploitation, it is not necessary to perform the work again and the rating could correspond to an evaluation of the necessary effort for each factor.

NOTE Exploitation consisting in applying scripts, it is expected that some factor values will be reduced from the identification phase, in particular "Elapsed Time" and "Expertise". For the same reason, the "Knowledge of the TOE" factor is not applicable in the exploitation phase (all the knowledge is scripted).

9.1.2. Factors to be considered

As in [CEM], the factors to be considered consist of ***Elapsed time***, ***Expertise***, ***Knowledge of the TOE***, ***Window of opportunity***, and ***Equipment***. But ***Window of opportunity*** is divided into two subfactors ***Window of opportunity (Access to the TOE)*** and ***Window of opportunity (Access to biometric characteristics)***.

Elapsed time is the total amount of time taken by the attacker.

In the identification phase, elapsed time corresponds to the time required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary hardware or software equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. One of the outputs from identification is, for instance, a script that gives a step-by-step description of how to carry out the attack. This script is assumed to be used in the exploitation part.

In the exploitation phase, elapsed time corresponds to the time necessary to apply the "script" to specific biometric characteristics. For example, for a presentation attack to a fingerprint capture device, it corresponds to the time required to create a PAI from an image of a print (and not the acquisition of this image which is taken into account in the factor ***Window of opportunity (Access to biometric characteristics)***).

Potential difficulties to have an access to the TOE in exploitation environment are taken into account in the factor ***Window of opportunity (Access to the TOE)***.

Expertise refers to the level of proficiency required by the attacker and the general knowledge that he possesses, not specific of the system being attacked. The levels are as follows:

a. *Layman* is the level no real expertise needed and such that any person with a regular level of education is capable of performing the attack. For example, creating a PAI in a known (published) way without specific difficulties (specific or difficult to buy materials) is considered at this level of expertise.

b. *Proficient* is the level such that some advanced knowledge in certain specific topics (biometrics) is required as well as good knowledge of the state-of-the-art of attacks. An attacker of this level is capable of adapting known attack methods to his needs. For example, adapting a known attack type (published) by the choice of specific (not published and sometimes difficult to find) materials in order to bypass a presentation attack detection mechanism and/or finding a non-evident way to present this PAI to the system can be considered at this level of expertise.

c. *Expert* is the level such that a specific preparation in multiple areas such as pattern recognition, computer vision or optimization is needed in order to carry out the attack. An attacker of this level is capable of generating his own new attacking algorithms. For example, finding a new (unpublished) way of creating an attack type using new and specific materials (unpublished) to counter an advanced presentation attack detection mechanism, can be considered at this level. In addition, this level can be associated with specific equipment (bespoke)

d. *Multiple Experts* is the level such that the attack needs the collaboration of several people with high level expertise in different fields (e.g., electronics, cryptanalysis, physics, etc.). It has to be noticed that a specific competence in biometrics is not considered as "multiple expertise". For example, building a "hill climbing" attack by gaining access to the comparison scores requires additional expertise to electrically attack and penetrate the TOE, which can be considered to constitute a "multi expertise" level.

NOTE As previously noted, exploitation expertise is usually lower than identification expertise. Layman or Proficient can be considered as typical value for expertise in the exploitation phase. For the same reason, the multiple expert level is excluded from the exploitation phase.

NOTE As all the factors, higher rating would require specific justifications from the evaluator.

Knowledge of the TOE refers to the amount of knowledge of system required to perform the attack. For instance, format of the acquired samples, size and resolution of acquisition systems, specific format of templates, but also specifications and implementation of countermeasures are knowledge that could be required to set up an attack.

This information could be publicly available at the website of the capture device manufacturer or protected (distributed to stakeholders under non-disclosure agreement or even classified inside the company). The levels are as follows:

a. *Public information* which is fairly easy to obtain (e.g., on the web).

b. *Restricted information* which is only shared by the developer and organizations which are using the system, usually under a non-disclosure agreement.

c. *Confidential information* which is only available within the organization that develops the system and is in no case shared outside it.

d. *Critical information* which is only available to certain people or groups within the organization which develops the system.

Special attention should be paid in this point to possible countermeasures that may be implemented in the system and whether it is necessary or not to have knowledge of their existence in order to be successful in a given attack.

It is assumed that all the knowledge required to perform the attack is gained during the identification phase and "scripted" for the exploitation. Therefore, this factor is not used for the exploitation phase.

Window of opportunity (Access to the TOE) refers to measuring the difficulty to access the TOE either to prepare the attack or to perform it on the target system.

For the identification phase, elements that should be taken into account include the easiness to buy the same biometric equipment (with and without countermeasures).

For exploitation phase, both technical (such known/unknown tuning) and organizational measures (presence of a guard, ability to physically modify the target, limited number of tries, etc.) should be taken into account.

The number and the level of equipment requested to build the attack is also taken into account in this factor.

This factor is not expressed in terms of time. The levels are as follows:

a. *Easy*: For identification phase, there is no strong constraint for the attacker to buy the TOE (reasonable price) to prepare its attack. For exploitation phase, there is no limit in the number of tries and the presentation attack is difficult to detect.

b. *Moderate*: For identification phase, specialised distribution schemes exist (not available to individuals). For exploitation phase, either a tuning of the attack for the final system is required (unknown parameterization of countermeasures for example) or there is a supervision of the biometric system emitting, for example, an alert in case of numerous fail presentations.

c. *Difficult*: For identification phase, the system is not available except for identified users and access requires compromising of one of the actors. For exploitation phase, for example PAIs must be adapted to the (unknown) specific tuning, or there is a strong supervision (for example a guard), or the system needs physical modification (for example physically accessing a hidden signal significant to the comparison score). Compromising one actor involved in the use of the system (guard, administrator, and maintenance) is often required.

Window of opportunity (Access to biometric characteristics) refers to measuring the difficulty to access the target biometric characteristics either to prepare the attack or to perform it on the target system

Security evaluations of [CC] are dedicated to evaluate the intrinsic resistance of a system. Due to the potential number of attack paths (with or without the cooperation of an enrolled subject for example) the evaluation does not take into account the way a real biometric characteristic is acquired. For presentation attack detection, the vulnerability analysis is based on the hypothesis that a real "image" is available, and the rating only concerns the creation and the presentation of a PAI.

However, it is important to be able to compare the resistance of various systems, even based on different biometrics. In addition, getting a real "image" to build a PAI is clearly part of an attack and it is of interest, for the final user of the TOE and the pertinence of a certificate to add a factor related to this aspect.

The levels are as follows:

a. *Immediate* is for 2D face, signature image, and voice. Samples of these modalities can be collected without difficulty, even without direct contact with an enrolled data subject (an exploration of the web and the social networks and so forth).

b. *Easy* is for fingerprint. Latent fingerprints are often left on objects the enrolled data subject had in hand, but need to be revealed, acquired and the corresponding images need a preprocessing.

c. *Moderate* is for 3D face, dynamic signature, and 3D fingerprint. 3D images require multiple acquisitions, probably in a controlled way, without the collaboration of an enrolled data subject but probably with a direct contact with them.

d. *Difficult* is for iris and vein. Iris images can be acquired with a high resolution camera, but with some difficulties to get a complete high quality image without the cooperation of an enrolled data subject. Veins are a hidden characteristic, but infra-red cameras, close to them, can acquire images to be used.

NOTE The above distribution of modalities per level is subject to modification depending on the evolution of technologies and usage. The current distribution is to be seen as guidance for the evaluator, who will have to adapt the rating to state-of-the-art.

NOTE Rating the resistance of a system is based on rating the successful attacks and verifying that no successful attack is found at the targeted level. Some attacks do not need real biometric data to be available, for example, attacks based on synthetic images or template generation. In such a case, this factor has to be considered to be *Immediate*.

Equipment refers to the type of equipment required to perform the attack. This includes the biometric databases used (if any). The levels are follows:

Standard equipment is an orderable, easy to obtain and simple to operate equipment (e.g., computer, video cameras, mobile phones, "do it yourself" material, and artistic leisure materials).

Specialised equipment refers to fairly expensive equipment, not available in standard markets and which require of some specific formation to be used (e.g., laboratory equipment, advanced printer specific materials and inks, and advanced oscilloscopes).

Bespoke equipment refers to very expensive equipment with difficult and controlled access; for example, research printing systems with specific ink definition and flexible support adaptation. In addition, if more than one specialised equipment is required to perform different parts of the attack, this value should be used. Before using this level, it has to be carefully checked that no service is available (renting, limited time access, etc.). If such service exists, the level has to be moved down to Specialised level.

9.1.3. Calculation of attack potential

Table 3, “Calculation of attack potential for general biometric system” identifies the factors discussed in the previous Section and associates numeric values with the total value of each factor.

Table 3. Calculation of attack potential for general biometric system

Factor	**Value**	
	Identification	Exploitation
Elapsed Time		
⇐ one day	0	0
⇐ one week	1	2
⇐ two weeks	2	4
⇐ one month	4	8
> one month	8	16
Expertise		
Layman	0	0
Proficient	2	4
Expert	4	8
Multiple experts	8	Not applicable
Knowledge of TOE		
Public	0	Not applicable

Factor	Value	
Restricted	2	Not applicable
Sensitive	4	Not applicable
Critical	8	Not applicable
Window of Opportunity **(Access to TOE)**		
Easy	0	0
Moderate	2	4
Difficult	4	8
Window of Opportunity **(Access to Biometric Characteristics)**		
Immediate	Not applicable	0
Easy	Not applicable	2
Moderate	Not applicable	4
Difficult	Not applicable	8
Equipment		
Standard	0	0
Specialised	2	4
Bespoke	4	8

In order to calculate the attack potential value of the entire attack, the evaluator shall add all the values of all the factors in identification phase and exploitation phase.

9.1.4. Rating of vulnerabilities and TOE resistance

The "Values" column of Table 4, “Rating of vulnerabilities and TOE resistance” indicates the range of attack potential values (calculated using Table 3, “Calculation of attack potential for general biometric system”) of an attack scenario that results in the SFRs being undermined.

Table 4. Rating of vulnerabilities and TOE resistance

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
< 10	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-19	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
20-29	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
30-39	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
⇒ 40	Beyond-High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

9.2. Application notes for [BIOPP-Module]

Attack potential table Table 3, “Calculation of attack potential for general biometric system” defined in previous Section doesn’t consider specific restrictions introduced by [BIOPP-Module]. For example, [BIOPP-Module] assumes that allowable maximum number of unsuccessful authentication attempts is limited that influence the calculation of ***Window of Opportunity (Access to TOE)*** for exploitation phase.

The evaluator shall take following application notes into account to calculate the attack potential for [BIOPP-Module], especially calculating the attack potential for presentation attacks during performing EAs for FIA_MBV_EXT.3.

9.2.1. Application note for Window of Opportunity (Access to TOE) for Identification

The evaluator shall select “Easy” because the TOE is the mobile device that anyone can purchase.

9.2.2. Application note for Window of Opportunity (Access to TOE) for Exploitation

The evaluator shall select “Difficult” because number of unsuccessful authentication attempts for mobile biometric verification is limited, and mobile biometric verification become unusable if the number of failure attempts exceed the limit.

9.3. Pass/Fail criteria for EAs for FIA_MBV_EXT.3

As required by CC, the evaluator shall determine that the TOE is resistant to an attacker possessing a Basic attack potential based on Table 3, “Calculation of attack potential for general biometric system”. However, the table doesn’t provide any guidance for the probability of success or failure of presentation attack.

The evaluator may have enough confidence to assign fail verdict to the TOE if the evaluator find the PAIs that succeed the attack repeatably or at high probability (e.g. almost 100%).

However, the evaluator can’t make an objective decision if the probability of success decreases at certain level because the mobile device limits the number of unsuccessful authentication attempts for mobile biometric verification and the attacker can’t present the PAI to the TOE so many times in the actual operational environment.

This Section provides the Pass/Fail criteria for EAs for FIA_MBV_EXT.3 taking this particular aspect into account so that the evaluator can make consistent and objective decision.

9.3.1. Pass/Fail criteria

The mobile device limits the number of unsuccessful authentication attempts for mobile biometric verification, as required by [MDFPP]. Therefore, the attacker must succeed the presentation attack at least one time within this limit.

This SD assumes that the attacker actually performs the presentation attack only if the attacker can create the “Reliable PAIs”. “Reliable PAIs” are those PAIs that succeed at least one attack within the allowable number of attempts (i.e. succeed to unlock the mobile device) at more than 80% of probability. This SD selects this probability based on the use case assumed in [BIOPP-Module].

The probability of a successful presentation attack for one attempt $\boldsymbol{p}$ needs to satisfy the following equation to satisfy the above condition.

$1-(1-\boldsymbol{p})^{\mathbf{n}} > 0.8$ (**n** = allowable number of unsuccessful attempts)

The following table shows that example of pairs (maximum ***p*** for particular **n**) that satisfy the above equation.

Table 5. Example of (n, p) pair

n	***p***
4	0.33 (33%)
6	0.23 (23%)
8	0.18 (18%)

The evaluator shall set **n** based on the assignment in FIA_AFL_EXT.1 in the ST that claim conformance to [MDFPP]. If the ST assign 5 to the maximum number of unsuccessful attempts for mobile biometric verification, **n** should be 5. If the ST states that this number is configurable from 5 to 10, the evaluator shall assume the worst-case scenario and **n** should be 10.

The evaluator shall assign pass verdict to the TOE only if the evaluator can’t find those PAIs that the probability of successful attack is more than ***p***.

The evaluator shall make at least 3 PAIs from three test subjects following the same creation process and perform at least 10 attempts for each PAI to calculate ***p*** (i.e. minimum number of attempts for calculation of ***p*** for each PAI is 3 * 10 = 30).

The evaluator should focus on a few PAIs that show highest error rate at the independent testing or hold highest quality for the penetration testing and spend enough time for training before conducting the final testing to measure ***p*** for those PAIs.

9.3.2. Additional application notes for AGD Class for FIA_MBV_EXT.3

CEM work unit AGD_OPE.1-1 requires the evaluator to examine the AGD guidance to determine that it describes appropriate warnings for secure use of the TOE.

The evaluator shall examine that appropriate warnings is provided in the AGD guidance if the evaluator can find those PAIs that pass the penetration test however whose ***p*** is higher than 7%.

Those PAIs can succeed at least one presentation attack (and succeed to unlock the mobile device) at 25% of probability when allowable number of unsuccessful attempts is 4 (i.e. **n** = 4).

Example of warnings is that the AGD guidance may warn that the mobile biometric verification is less secure than a password and recommend using a password for security sensitive services.

10. References

[BIOPP-Module] collaborative PP-Module for Mobile biometric enrolment and verification - for unlocking the device –, May 01, Version 0.8, 2019

[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

[ISO/IEC 15408-4] Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities, under development.

[ISO/IEC 19792] Security evaluation of biometrics, First edition.

[ISO/IEC 19795-1] Biometric performance testing and reporting - Part 1: Principles and framework, First edition.

[ISO/IEC 19795-2] Biometric performance testing and reporting - Part 2: Testing methodologies for technology and scenario evaluation, First edition.

[ISO/IEC 19795-3] Biometric performance testing and reporting - Part 3: Modality-specific testing, First edition.

[ISO/IEC 19989-1] Criteria and methodology for security evaluation of biometric systems – Part 1: framework, under development.

[ISO/IEC 19989-2] Information technology - Security techniques - Criteria and methodology for security evaluation of biometric systems - Part 2: Biometric recognition performance

[ISO/IEC 21879] Performance testing of biometrics on mobile devices

[ISO/IEC 30107-1] Biometric presentation attack detection — Part 1: Framework, First edition.

[ISO/IEC 30107-3] Biometric presentation attack detection — Part 3: Testing and reporting, First edition.

[MDFPP] Protection Profile for Mobile Device Fundamentals, Version 3.2

[Toolbox] **TBD**