Supporting Document Mandatory Technical Document

Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOSD]

Version 2.1-PD1, January 7, 2026

Table of Contents

Foreword

This is a Supporting Document, intended to complement the Common Criteria (CC) CC:2022, Release 1 and Errata and Interpretation, Version 1.1, and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

This Supporting Document is a "Mandatory Technical Document", whose application is mandatory for evaluations and only those certificates issued as a result of its application are mutually 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 1.2, “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
0.4	August 5, 2019	Updates based on Public Review Draft 1 comments
0.5	December 5, 2019	Updates to make PAD optional
0.92	December 20, 2019	Public Review Draft 2
0.95	March 13, 2020	Proposed Release
1.0	May 11, 2020	Public Release
1.0.1	November 10, 2020	Technical Decision BIO0002
1.1	September 12, 2022	Incorporated TDs and NIAP comments for PP_MDF integration
2.0	February 28, 2025	Incorporated updated PAD levels and CC:2022 compliance
2.1-PD1	January 7, 2026	Updates to the Attacl Potential Table and PP-Modules for AVA_VAN

General Purpose

See Section 1.2.

Field of special use

This Supporting Document applies to the evaluation of TOEs claiming conformance with the collaborative PP-Module for 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.

Chapter 1. Introduction

1.1. Supporting Document Reference

Supporting Document Reference	Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOSD]
Supporting Document Version	2.1-PD1
Supporting Document Date	January 7, 2026
Toolbox Overvew Reference	Toolbox Overview
Toolbox Overview Version	2.1-PD1
Toolbox Overview Date	January 7, 2026

1.2. Technology Area and Scope of Supporting Document

This Supporting Document (BIOSD) defines the Evaluation Activities (EAs) associated with the collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module] that is intended for use with the Base-PP identified in the appropriate PP-Configuration.

This BIOSD 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 biometric enrolment and verification, and to the particular ways in which the TOE optionally needs to be assessed across a range of different artificial artefact instruments (specifically artificial, not natural, Presentation Attack Instruments). 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 BIOSD 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 Chapter 8, *Developer’s performance report and its assessment strategy*).

1.3. Structure of the Document

EAs can be defined for both SFRs and SARs. These are defined in separate sections of this BIOSD. EAs are intended to be both cost effective and practical.

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.

1.4. Terminology

1.4.1. Glossary

For definitions of standard CC terminology see [CC1]. For definitions of biometrics and the computer, see [BIOPP-Module] and the Base-PP.

1.4.2. Acronyms

Acronym	Meaning
BAF	Biometric Authentication Factor
BMD	Biometrics Management Description
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
EA	Evaluation Activity
FAR	False Accept Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
IAPAR	Imposter Attack Presentation Accept Rate
iTC	International Technical Community
NBAF	(Non-Biometric) Authentication Factor
NFIQ	NIST Fingerprint Image Quality
PAD	Presentation Attack Detection
PAI	Presentation Attack Instrument (artefact)

Acronym	Meaning
PP	Protection Profile
SAR	Security Assurance Requirement
BIOSD	Supporting Document
SEE	Separate Execution Environment
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TSFI	TOE Security Functions Interface
TSS	TOE Summary Specification

Chapter 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 BIOSD 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 BIOSD.

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 the Base-PP 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 of the TOE that the BIO-iTC has determined is necessary in the context of the associated SFR. 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 one’s NBAF. Security requirements for the NBAF mechanism are defined in the Base-PP and out of scope of this EA.

2.3.1.2. Dependency

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

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 to the biometric system

   AGD guidance may include online assistance, errors, prompts or warnings 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 one’s valid NBAF before the biometric enrolment.

2.3.1.5.2. Strategy for ATE_IND

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

1. The evaluator shall try to enrol without setting a NBAF and confirm that it is not possible to enrol.
2. The evaluator shall set a NBAF and confirm that enrolment is not possible without entering the NBAF 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 users authenticated by a NBAF can enrol 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

Biometric verification performance depends on quality of samples from which templates are generated. The evaluator shall examine that the TOE checks the quality of samples to create enrolment and authentication templates based on the assessment criteria so that the TOE can 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 are not 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 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

   - If standard quality metrics are selected and assigned, the TSS shall include information (e.g. name of quality metrics and section numbers that define the metrics in the standard) to identify quality metrics that the TOE implements
   - If a developer defined quality assessment is selected, the TSS shall include an overview of the quality metrics used for the assessment

b. The BMD should provide information about the assessment criteria that explains how the TOE checks the quality of samples to create enrolment and authentication templates. The assessment criteria for enrolment templates may include the following information

   - Quality requirements for the biometric sample to ensure that a sufficient amount of distinctive features are available
   - Method to quantify the quality of samples (e.g. method to generate quality score)
   - Assessment criteria to accept the sample of sufficient quality (e.g. compare quality score to quality threshold)
   - Quality standard that the TOE uses to perform the assessment if the TOE follows such standard (e.g. ISO/IEC 29794-4 for fingerprint)

   The assessment criteria for authentication templates may include additional criteria for creation of authentication templates in addition to above points.

   The BMD can make a priori assumptions about the usefulness or efficacy of the criteria or metrics. If standard quality metrics are assigned, the BMD may refer to the standard that defines quality metrics. If developer defined quality assessment is selected, the BMD shall provide the same level of information about the assessment criteria as the standard (e.g. ISO/IEC 29794-4 for fingerprint) does.

c. The BMD shall also provide information about how authentication templates are created and, where applicable, updated. The information shall be detailed enough to conduct the EA for authentication template described below.

d. AGD guidance shall provide clear instructions for a user to enrol to the biometric system

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

e. If supplementary information is provided in addition to the information provided in b), (the quality assessment criteria report explained in Chapter 10, *Developer's quality assessment criteria report of biometric samples*) shall describe the efficacy of quality metrics, how the efficacy is tested or confirmed and how the low-quality samples can be generated

2.3.2.5. Assessment Strategy

2.3.2.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

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

The evaluator shall examine the quality assessment criteria report to check the efficacy of quality metrics to confirm that the TOE can select enough quality of samples from which the TOE generates templates of sufficient quality.

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

1. The evaluator shall perform biometric enrolment that results in creation of samples from which templates will be created that do not satisfy the assessment criteria described in quality assessment criteria report. Methods to create low-quality samples are described in the report (e.g. varying temperature / humidity conditions of the finger skin, low physical pressure, too less presentation time or incorrect finger positioning angles for fingerprint verification)
2. The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that the TOE does not create enrolment templates from samples that do not meet the assessment criteria specified in the quality assessment criteria report
3. The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that any enrolment templates are created by TOE from samples that meet the assessment criteria specified in the quality assessment criteria report correctly

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

1. The evaluator shall enrol to the biometric system
2. The evaluator shall present biometric samples repeatedly to trigger the TOE to create authentication templates
3. The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that the TOE does not create authentication templates from samples that do not meet the assessment criteria specified in the quality assessment criteria report
4. The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that any authentication templates created by TOE from samples that meet the assessment criteria specified in the quality assessment criteria report correctly

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, BMD, AGD guidance and the quality assessment criteria report

b. The TOE creates only templates from samples that pass the quality 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 biometric verification mechanism whose upper bound confidence interval of error rates does not exceed 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 report explained in Chapter 8, *Developer's performance report and its assessment strategy*) to achieve this objective following instruction defined in Assessment Strategy. The [BIOPP-Module] assumes that the biometric verification is not used for security sensitive services and the TOE operational environment also limits the maximum number of failed verification attempts in succession. Therefore, the evaluator does not need to gather large quantities of test subjects to conduct the independent testing for this SFR.

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 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. BMD shall provide information about how the upper bound confidence interval of error rates are estimated

    - The BMD may refer to the developer's performance report

c. AGD guidance shall provide clear instructions for a user to verify one's biometric to unlock the computer

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

d. Supplementary information (developer's performance report) shall describe the developer's performance test protocol and result of testing

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 and BMD to understand how the TOE verifies a user with one's biometric characteristics. The evaluator shall also examine the guidance about how the TOE supports a user to verify one's biometric correctly and how the TOE behaves when biometric verification is succeeded or failed.

The evaluator shall examine developer's performance report to verify that the developer conducts the objective and repeatable performance testing. Minimum requirements for conducting performance testing are defined in Chapter 8, *Developer's performance report and its assessment strategy*.

Requirements defined in Chapter 8, *Developer's performance report and its assessment strategy* are based on 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 report meets all requirements in Chapter 8, *Developer's performance report and its assessment strategy* and seek a rationale if the developer's performance report does not meet any requirements and determine whether the rationale is valid or not.

Finally, the evaluator shall check that the estimated upper bound confidence interval of error rates (FRR/FAR or FNMR/FMR) reported in the developer's performance report do not exceed the claimed 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, BMD and AGD guidance

b. Developer’s performance report meets all requirements in Chapter 8, *Developer’s performance report and its assessment strategy* and a valid rationale is provided by developer if the developer’s performance report doesn’t meet any requirements

c. Upper bound confidence interval of error rates (FRR/FAR or FNMR/FMR) reported in the developer’s performance report do not exceed the claimed error rates specified in FIA_MBV_EXT.1.2

2.3.3.7. Requirements for reporting

The evaluator shall report the summary of the 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 the developer’s performance report does not meet any requirements in Chapter 8, *Developer’s performance report and its assessment strategy*.

2.3.4. EA for FIA_MBV_EXT.2

2.3.4.1. Objective of the EA

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 are 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 samples for enrolment defined in Section 2.3.2, “EA for FIA_MBE_EXT.2” and samples for verification defined in this section may not be the same. Assessment criteria for samples for enrolment may be stricter than the one for samples for verification defined in this section.

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 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
   - If standard quality metrics are selected and assigned, the TSS shall include information (e.g. name of quality metrics and section numbers that define the metrics in the standard) to identify quality metrics that the TOE implements
   - If a developer defined quality assessment is selected, the TSS shall include an overview of the quality metrics used for the assessment

b. The BMD should provide information about the assessment criteria that explains how the TOE checks the quality of samples for biometric verification. The assessment criteria for biometric verification may include the following information

   - Quality requirements for the biometric sample to ensure that a sufficient amount of distinctive features are available
   - Method to quantify the quality of samples (e.g. method to generate quality score)
   - Assessment criteria to accept the sample of sufficient quality (e.g. compare quality score to quality threshold)
   - Quality standard that the TOE uses to perform the assessment if the TOE follows such standard (e.g. ISO/IEC 29794-4 for fingerprint)

   The BMD can make a priori assumptions about the usefulness or efficacy of the criteria or metrics. If standard quality metrics are assigned, the BMD may refer to the standard that defines quality metrics. If developer defined quality assessment is selected, the BMD shall provide the same level of information about the assessment criteria as an equivalent image quality standard for the specific modality (e.g. ISO/IEC 29794-4 for fingerprint) does.

c. AGD guidance shall provide clear instruction for a user to verify one’s biometric

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

d. If supplementary information is provided in addition to the information provided in b), (the quality assessment criteria report explained in Chapter 10, *Developer’s quality assessment criteria report of biometric samples*) shall describe the efficacy of quality metrics, how the efficacy is tested or confirmed and how the low-quality samples can be generated

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 and BMD to understand how the TOE checks quality of samples captured. The evaluator shall also examine the AGD guidance about how the TOE supports a user to verify correctly and how the TOE behaves when low quality samples are presented to the TOE for verification.

The evaluator shall examine the quality assessment criteria report to check the efficacy of quality metrics to confirm that the TOE can select enough quality of samples from which the TOE generates templates of sufficient quality.

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

1. The evaluator shall present biometric low-quality samples for biometric verification that do not satisfy the assessment criteria described in quality assessment criteria report. Methods to create low-quality samples are described in the report (e.g. varying temperature / humidity conditions of the finger skin, low physical pressure, too less presentation time or incorrect finger positioning angles for fingerprint verification)
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 do not meet the assessment criteria specified in the quality assessment criteria report
3. The evaluator shall check the TOE internal data (e.g. quality scores and quality threshold) to confirm that any samples accepted by TOE meet the assessment criteria specified in the quality assessment criteria report correctly

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, BMD, AGD guidance and quality assessment criteria report

b. The TOE accepts only samples that pass the quality assessment criteria for biometric verification through the independent testing

2.3.4.7. Requirements for reporting

The evaluator shall report the summary of the 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_PAD_EXT.1

2.3.5.1. Objective of the EA

The evaluator shall verify the support for PAD in the TOE, and if PAD is supported, the specific level of PAD which can be detected.

2.3.5.2. Dependency

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

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_PAD_EXT.1 at high level description

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 to understand what type of PAD is supported by the TOE.

Guidance and usage is evaluated through FIA_MBE_EXT.3 and FIA_MBV_EXT.3.

2.3.5.5.2. Strategy for ATE_IND

For a TOE providing PAD support testing is covered through FIA_MBE_EXT.3 and FIA_MBV_EXT.3 as claimed.

2.3.5.6. 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 claimed PAD level for verification is equal to or higher than the claimed PAD level for enrolment

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 computer provides the Separate Execution Environment (SEE), an operating environment separate from the main computer 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. In addition to providing the SEE, it is assumed that the computer provides a secure method to transmit data between the associated components and the SEE, such as the biometric capture sensor.

Evaluation of this SEE is out of scope of [BIOPP-Module] and the evaluator does not need to evaluate this environment itself. However, the evaluator shall examine that the TOE processes any plaintext biometric data within the boundary of the SEE, and that the transmission of this data is via a channel protected from the main computer operating system. The SEE is responsible for preventing any entities outside the environment from accessing plaintext biometric data.

While the TOE operates inside the SEE, it is possible that TSFIs may exist within the product that could be used for exporting plaintext data locally. These could exist for production functionality or as part of debug capabilities (such as those provided within an SDK). In the evaluated configuration, there must not be any method for exporting plaintext biometric data from the TOE, and so these interfaces must be controlled for this purpose, such as by admin control or by disabling or removing them from the production device.

FPT_BDP_EXT.1 applies to plaintext biometric data being processed during biometric enrolment and verification. Protection of stored and externally transmitted biometric data is out of scope of this EA and covered by modified FPT_KST_EXT.1 and FPT_KST_EXT.2 defined in [BIOPP-Module] respectively.

2.4.1.2. Dependency

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

2.4.1.3. Tool types required to perform the EA

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

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

b. TSS or BMD shall provide additional details about the protection mechanisms provided by the SEE and environment

c. TSS or BMD shall provide details about TSFIs that may provide the capability to export plaintext biometric data but which must be disabled/blocked for use in the evaluated configuration

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 are captured by a biometric capture sensor and then sent to the processors in the computer for signal processing, PAD and comparison and the decision outcome is returned. This is a typical process flow of biometric verification; however, a biometric capture sensor may do all the tasks within the sensor. In either case, all TSF modules (i.e. biometric capture sensor and any software running in biometric capture sensor and the computer 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 case, the evaluator shall examine the TSS to confirm that;

a. All TSF modules and physical interconnections are within the defined boundary of the SEE and any entities outside the SEE including the main computer operating system can’t interfere with transmission between and processing of these modules

b. All plaintext biometric data (whether generated by the biometric capture sensor or by the evaluation processes of the TSF) is retained in volatile memory within the SEE and any entities outside the SEE including the main computer operating system can't access these data. Any TSFIs which may exist, do not reveal plaintext biometric data to any entities outside the SEE. The evaluator shall examine TSFIs of TSF modules provided by the biometric capture sensor (e.g. SDK) because they may include testing or debug codes and the developer who integrated the sensor into the TOE may apply changes to those modules

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 and BMD 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 and BMD to seek for a logical explanation how the above criteria are 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 and BMD

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.

2.4.1.7.1. Strategy for ATE_IND

Plaintext biometric data must not be accessible from any entities outside the SEE, especially the main computer operating system, to meet FPT_BDP_EXT.1. This means that:

a. The TOE must not expose the plain biometric data to the memory that is accessible by the main computer operating system during the processing of biometric data.

b. Any TSFIs identified in the TSS that can output plaintext biometric data must not be accessible by the main computer operating system for local storage.

From a testing perspective, a) is a function of ensuring the TOE design such that it is contained within the SEE boundaries. As the SEE itself is out of scope, there is no specific test to verify this as it brings the SEE itself into the scope of the testing (as if the TOE design is correct any failure would be due to an SEE failure).

If the TSS describes any TSFIs that may export plaintext biometric data (such as those provided by an SDK for integration and debugging), the evaluator must verify that b) is true.

If it is impractical or inadequate to conduct the following tests, the developer may propose alternate approaches to verify them. It is the evaluator's responsibility to determine the suitability of an alternate approach. For example, an analysis of source code to determine that they are met by the TOE is an acceptable alternate approach, as described in the [CEM].

a. TSFI invocation test

If TSFIs exist, they could be used to output plaintext biometric data to the operating system, and so the evaluator shall perform this test. The following test steps require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

1. The evaluator shall identify any TSFIs that output plaintext biometric data to the memory that is accessible by the operating system.
2. The evaluator shall attempt to access and TSFIs using the developer provided test platform and tools to verify that no plaintext data can be accessed from the main computer operating system.

2.4.1.8. 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 BMD

b. The TOE does not provide access to the biometric transaction to the main computer operating system

c. No TSFIs provide access to plaintext biometric data to the main computer operating system

2.4.1.9. 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_PBT_EXT.1

2.4.2.1. Objective of the EA

Only an authenticated user can add one’s own templates during biometric enrolment as defined in the FIA_MBE_EXT.1 and those templates are not stored as plaintext as required by the modified FPT_KST_EXT.1 defined in the [BIOPP-Module]. However, the TOE may provide functions (e.g. revocation of templates) to access the templates. The evaluator shall confirm that only an authenticated user using a NBAF as specified by the ST author can access the templates through the TSFI provided by the TOE.

2.4.2.2. Dependency

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

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_PBT_EXT.1 at high level description

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

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 TSFI through which the user can access (e.g. revoke) the templates. The evaluator shall confirm that those TSFI requires using a NBAF as specified by the ST author.

2.4.2.5.2. Strategy for ATE_IND

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

1. The evaluator shall perform functions through the TSFIs that access the templates
2. The evaluator shall check that the TSFI requires using a NBAF as specified by the ST author
    a. The evaluator shall attempt to add new, change and remove existing BAFs on the TOE and ensure the NBAF is required before allowing any change

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

b. The TOE protects the templates using a NBAF as specified by the ST author

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.

Chapter 3. Evaluation Activities for PP_MDF Requirements

In addition to the EAs required by the Base-PP, the evaluator shall perform the following additional EAs to ensure that the Base-PP’s security functionaltiy is maintained by the addition of the PP-Module.

3.1. Modified SFRs from the Base-PP

3.1.1. Cryptographic Support (FCS)

3.1.1.1. FCS_CKM_EXT.4 Key Destruction

Refer to the EA for FCS_CKM_EXT.4 in the [PP_MDF] including biometric data as critical security parameters for the EA.

3.1.2. Protection of the TSF (FPT)

3.1.2.1. FPT_AEX_EXT.4 Domain Isolation

Refer to the EA for FPT_AEX_EXT.4 in the [PP_MDF] including the protection of biometric data in the isolation description.

3.1.2.2. FPT_KST_EXT.1 Key Storage

Refer to the EA for FPT_KST_EXT.1 in the [PP_MDF] including biometric data as part of the plaintext key materials.

3.1.2.3. FPT_KST_EXT.2 No Key Transmission

Refer to the EA for FPT_KST_EXT.2 in the [PP_MDF] including biometric data as part of the plaintext key materials.

Chapter 4. Evaluation Activities for Selection-Based Requirements

4.1. Identification and Authentication (FIA)

4.1.1. EA for FIA_MBE_EXT.3

4.1.1.1. Objective of the EA

The evaluator shall verify that the TOE prevents use of artificial artefacts during biometric enrolment. This section defines EAs derived from ASE_TSS.1, AGD_OPE.1 and ADV_FSP.1.

The main part of EA for FIA_MBE_EXT.3 is evaluator's testing using the artefact. Chapter 7, *Evaluation Activities for PAD testing* defines EAs for ATE_IND.1 and AVA_VAN.1 in detail that the evaluator shall perform for PAD testing during the biometric verification. The same EAs can be applied to PAD testing during the biometric enrolment.

4.1.1.2. Dependency

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

4.1.1.3. Tool types required to perform the EA

No tool is required for this EA.

4.1.1.4. 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.3 at high level description. TSS may only state that the TOE implements PAD mechanism and may not disclose any information about the PAD mechanism itself in detail because such information may also be exploited by attackers

b. BMD shall provide additional information needed to explain the PAD mechanism within the scope of the assurance level claimed by [BIOPP-Module]

c. AGD guidance may provide information about how the TOE reacts when the artefact is detected

4.1.1.5. Assessment Strategy

4.1.1.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS, BMD and AGD guidance to check that the TSS, BMD or AGD guidance states that the TOE prevents the use of the artefact during biometric enrolment.

4.1.1.5.2. Strategy for ATE_IND

The main part of the EA is the evaluator's testing defined in Chapter 7, *Evaluation Activities for PAD* *testing*. The evaluator should not require a detailed design description of PAD from the developer because it's beyond the scope of assurance level claimed in [BIOPP-Module].

4.1.1.6. Pass/Fail criteria

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

a. TSS, BMD or AGD guidance states that the TOE prevents the use of the artefact during biometric enrolment

4.1.1.7. 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.

4.1.2. EA for FIA_MBV_EXT.3

4.1.2.1. Objective of the EA

The evaluator shall verify that the TOE prevents use of artificial artefacts during biometric verification. This section defines EAs derived from ASE_TSS.1, AGD_OPE.1 and ADV_FSP.1.

The main part of EA for FIA_MBV_EXT.3 is the evaluator's testing using the artefact. The Chapter 7, *Evaluation Activities for PAD testing* defines EAs for ATE_IND.1 and AVA_VAN.1 in detail that the evaluator shall perform during the testing.

4.1.2.2. 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 biometric enrolment and verification can be done correctly.

4.1.2.3. Tool types required to perform the EA

No tool is required for this EA.

4.1.2.4. Required input from the developer or other entities

Following input is required from the developer.

a. TSS shall explain how the TOE meets FIA_MBV_EXT.3 at high level description. TSS may only state that the TOE implements PAD mechanism and may not disclose any information about the PAD mechanism itself in detail because such information may also be exploited by attackers

b. BMD shall provide additional information needed to explain the PAD mechanism within the scope of the assurance level claimed by [BIOPP-Module]

c. AGD guidance may provide information about how the TOE reacts when the artefact is detected

4.1.2.5. Assessment Strategy

4.1.2.5.1. Strategy for ASE_TSS and AGD_OPE/ADV_FSP

The evaluator shall examine the TSS and AGD guidance to check that the TSS, BMD or AGD guidance states that the TOE prevents the use of the artefact during biometric verification.

The main part of the EA is the evaluator's testing defined in Chapter 7, *Evaluation Activities for PAD testing*. The evaluator should not require a detailed design description of PAD from the developer because it's beyond the scope of assurance level claimed in [BIOPP-Module].

4.1.2.6. Pass/Fail criteria

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

a. TSS, BMD or AGD guidance states that the TOE prevents the use of the artefact

4.1.2.7. 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.

Chapter 5. Evaluation Activities for Optional Requirements

The [BIOPP-Module] does not contain any optional requirements.

Chapter 6. Evaluation Activities for SARs in PP_MDF

[PP_MDF] and this BIOSD define Evaluation Activities for how to evaluate individual SFRs as they relate to the SARs for ASE_TSS.1, AGD_OPE.1, and ATE_IND.1.

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

6.1. Class ASE: Security Target

[PP_MDF] does not define any EAs and there is no additional EAs for [BIOPP-Module].

6.2. Class ADV: Development

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

6.3. Class AGD: Guidance Documentation

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

6.3.1. 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 [PP_MDF] and the operational guidance does not need to describe the security measures to be followed in order to fulfil the security objectives for the operational environment derived from those assumptions.

6.3.2. 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 is deemed satisfied for [BIOPP-Module].

6.4. Class ALC: Life-cycle Support

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

6.4.1. Application note for EA of ALC_CMC.1

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

6.5. Class ATE: Tests

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

6.5.1. Application note for EA of ATE_IND.1

The evaluator shall follow the same EAs defined in [PP_MDF] and the BIOSD.

6.6. Class AVA: Vulnerability Assessment

The evaluator shall take the following additional application notes into account to perform EAs defined in [PP_MDF] for [BIOPP-Module] when PAD testing is included in the evaluation. As PAD is an optional set of requirements, the vulnerability assessment activities related to PAD are only included when PAD is included.

6.6.1. Application note for EA of AVA_VAN.1

The evaluator shall follow the same EAs defined in [PP_MDF] and the BIOSD. As explained in the Chapter 7, *Evaluation Activities for PAD testing*, details of PAD testing for ATE_IND.1 are defined in [Toolbox].

Chapter 7. Evaluation Activities for PAD testing

7.1. Introduction

PAD is an optional set of requirements, when FIA_MBE_EXT.3 or FIA_MBV_EXT.3 are included in an evaluation. This set of Evaluation Activities are only performed if any of these requirements are included. PAD is measured using the Imposter Attack Presentation Attack Rate (IAPAR). IAPAR is a measure applied to a "full system" evaluation, not a component evaluation. Because the measure applies to the system as a whole, reasons for failure, such as presentation attack or sample dissimilarity, are not distinguished. According to ISO/IEC 30107-3, the proportion of presentation attacks using the same PAI species that result in an accepted verification is measured by IAPAR[1].

The evaluator shall perform the following two types of EAs or testing to evaluate the FIA_MBE_EXT.3 (Presentation attack detection for biometric enrolment) and FIA_MBV_EXT.3 (Presentation attack detection for biometric verification). The following section defines EAs for FIA_MBV_EXT.3 however, the evaluator can replace "verification" with "enrolment" and apply the EAs to FIA_MBE_EXT.3.

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, BMD or AGD guidance because [BIOPP-Module] does not require a formal or complete specification of PAD interface.

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

Instead, this BIOSD requires the evaluator to conduct ATE_IND.1 evaluation (i.e. independent testing) in a black-box manner. However, the problem of black-box testing for PAD, as described in ISO/IEC 30107-3, is that it is very difficult to have a comprehensive model of all possible artefacts. Therefore, it may be possible that different evaluators could use a different set of artefacts and see different test results for the same TOE.

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

The [Toolbox] includes a collection of test items for each biometric modality. Each test item describes the procedure to create artefacts 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, the [Toolbox] should be used in a different manner for AVA_VAN.1 evaluation. The following section explains how the [Toolbox] should be used in EAs for ATE_IND.1 and AVA_VAN.1.

7.1.1. Presentation Attack Instrument (artefact) species

There are many types of Presentation Attack Instruments that can be used to test a PAD subsystem. The [BIOPP-Module] specifically defines the artefacts that are to be used as artificial, and not natural. Natural artefacts, such as a dead eye, are not considered in scope for this evaluation. When searching for new artefact species, only artificial species should be considered.

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

7.2.1. Independent test activities using Toolbox

As described in previous section, the [Toolbox] defines test items to create a representative set of artefacts that the evaluator shall use for the testing. During ATE_IND.1 evaluation, the evaluator shall conduct all test items in the [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.

The developer needs to assign the maximum IAPAR in FIA_MBV_EXT.3. The evaluator shall follow the information in the [Toolbox], for example, the number of artefact presentations, to conduct the testing and confirm that measured IAPARs for all artefacts are equal to or less than the assigned IAPAR through the independent testing.

During the independent testing, the evaluator may find artefacts that are incorrectly matched to the enroled target user. However, the evaluator may not be able to reliably reproduce a successful presentation attack. The evaluator shall assign a fail verdict only if the evaluator can reproduce the artefact of which IAPAR is higher than the maximum value reliably and repeatably.

Those artefacts of which IAPAR is less than the maximum value but show one or more successful imposter presentations will be tested again during the AVA_VAN.1 evaluation.

The developer can select any biometric modalities in FIA_MBV_EXT.1 (corresponding test instructions for each modality are included in the [Toolbox]). If the developer wants to evaluate modalities not currently included in FIA_MBV_EXT.1, the developer and evaluator shall contact the BIO-iTC to work together to add the new modality and extend the [Toolbox]. Upon the BIO-iTC approval of this extension, the evaluator can proceed with PAD evaluation for the new modality.

7.2.2. 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.

The [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). The [Toolbox] also includes information that support the evaluator’s decision (ATE_IND.1-7).

7.3. EA for AVA_VAN.1 (Vulnerability survey)

7.3.1. 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.

7.3.1.1. Search for new artefacts

Each of the supported biometric modalities have a specific set of defined artefacts species in the [Toolbox] to be used in testing. These are devised based on publicly available information published by the publication date of the [Toolbox]. The BIO-iTC also verifies that test items cover all existing artefact species that are within the scope of Basic attack potential defined in Chapter 11, *Attack Potential and TOE resistance*.

However, new artefacts species may be found after the [Toolbox] is published. The evaluator shall search publicly available information that is published after the publication date of the [Toolbox] to look for new artefact species. New artefact species are those artefacts that are significantly different from, or made using significantly different materials than those covered by the [Toolbox], but still meet basic attack potential.

Those new artefact species that can be made by slightly modifying test items in the [Toolbox] are covered by the normal test plans.

7.3.1.2. New artefact Toolbox updates

To utilize new artefacts, they must have approval from the BIO-iTC through publication in an incremented toolbox version for the evaluator to evaluate against.[2] The evaluator shall report to the BIO-iTC when new artefact species are found so the artefacts may be added to the [Toolbox]. The requirements for addition of new artefact species can be found at the Biometrics Security home page. The new artefact species will be included as part of the [Toolbox] by the BIO-iTC and the evaluator must refer the latest [Toolbox] at the time of the evaluation.

7.3.1.3. Produce test plan

The evaluator shall select those artefacts that show higher IAPAR at the independent testing. The evaluator shall test them extensively during the penetration testing.

If there are no such artefacts, the evaluator should select “higher quality” artefacts. “Higher quality” means that artefacts are closer in resemblance to the biometric characteristics of the target user (e.g. higher resolution photo for face artefact). The evaluator may measure the quality score of samples captured from artefacts and select ones that produce higher scores as “higher quality” artefacts.

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

a. Modify the creation process of artefacts

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

   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 artefact (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 artefacts with clearer vein pattern for the penetration testing.

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

b. Change test subjects

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

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

c. Improve presentation method

   The evaluator may also increase time for artefact 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 artefact and sensor, and how to present the artefact to the TOE. However, it’s not possible for the evaluator to know the best distance or presentation method for the artefact in advance because this BIOSD requires the evaluator to test the TOE in a black-box manner. The evaluator may simply increase the number of attempts to find the best distance or presentation through trial and error process.

7.3.1.4. Conduct the penetration testing

The evaluator shall conduct the penetration testing based on the test plan.

The evaluator shall select those artefacts that may succeed the attack at higher probability as described in Section 7.3.1.3, “Produce test plan” for the penetration testing.

In order to place bounds on the effort involved related to the attack potential calculations for PAD functionality, the penetration testing is expected to be finished within a single week, considering the assurance level claimed by [BIOPP-Module].

7.3.1.5. Determine Pass/Fail of penetration testing

The evaluator shall assign a fail verdict if the evaluator can find the artefact where the IAPAR is higher than the maximum IAPAR and it can be reproduced reliably and repeatably by an attacker possessing a Basic attack potential.

7.3.2. 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 7.3.1.1, "Search for new artefacts" complements evaluator's action for searching publicly available information and identifying potential vulnerabilities (e.g. new artefact) (AVA_VAN.1-3, AVA_VAN.1-4 and AVA_VAN.1-5).

EAs in Section 7.3.1.3, "Produce test plan" and Section 7.3.1.4, "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 7.3.1.5, "Determine Pass/Fail of penetration testing" provides specific guidance for pass or failure of the testing (AVA_VAN.1-10).

[1] The 2017 edition defines this as Imposter Attack Presentation Match Rate (IAMPR) but this will be changed to IAPAR in a later revision.

[2] Publication can occur rapidly, typically ≤2 weeks

Chapter 8. Developer’s performance report and its assessment strategy

This Section describes requirements for the developer’s performance report and its assessment strategy.

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

The evaluator shall examine the performance report 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 ISO/IEC 19795-1 and ISO/IEC19795-2.

8.1. Requirements for the performance report

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

The performance report is most likely a separate confidential document and not part of the ST for public release.

8.2. Summary of contents

Table 2, “Reporting items” shows items that shall be reported in the performance report. The name or structure of performance report does not need to follow Table 2, “Reporting items”. However, all items in Table 2, “Reporting items” shall be written somewhere in the performance report. Also, if some items are not included in the performance report, the developer shall provide a rationale for such exclusion to the evaluator.

Table 2. Reporting items

Section	Item
Section 8.3.1	Overview of the performance testing
Section 8.3.2	Target application and influential factors
Section 8.3.3	Test subject selection
Section 8.3.4	Test instructions and training
Section 8.3.5	Test subject management
Section 8.3.6	Test procedure

8.3. Reporting items description

This Section describes each item in Table 2, “Reporting items” in detail. All items are created based on ISO/IEC 19795-1 and ISO/IEC19795-2 however some of them are modified to adjust to the CC evaluation.

8.3.1. Overview of the performance testing

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

a. Performance test configuration

   The performance report 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 identifies the TOE shall be reported. [BIOPP-Module] is intended to be used with the Base-PP and reference for the computer can be used as the TOE reference only if the reference for the computer also uniquely identifies the biometric system embedded in the computer

      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 does not affect the TOE performance shall also be provided. For example, the developer may claim that the performance is not affected because modified code is not executed during biometric verification or the developer may run regression tests to verify that modification does not change the result of verification (e.g. similarity score).

   2. TOE configuration

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

   3. Type of verification algorithm

      Type of verification algorithm, symmetric or asymmetric, shall be provided. As explained in Section 9.1.5, “Cross-comparison for FAR/FMR”, cross-comparison of attempts/templates of ordered pairs is not allowed for symmetric verification algorithm.

   4. Performance test tools

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

b. Result of the performance testing

   The performance report 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 biometric verification

   The performance testing shall be done for all modalities selected in FIA_MBV_EXT.1. The results 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 performance report shall clearly define what constitutes the transaction based on the guidance provided in Chapter 9, *Requirement for the number of test subject, 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 Chapter 9, *Requirement for the number of test subject, 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 not 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.

     Note all test subjects may not 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

   - Estimation method for confidential interval

The upper bound of the confidence interval of error rates (e.g. FAR and FRR) selected at FIA_MBV_EXT.1.2 shall be estimated and reported. The method of estimation shall follow the methods defined in Annex B of ISO/IEC 19795-1.

ISO/IEC 19795-1 explains estimation methods for confidence interval for FMR and FNMR. However, ISO/IEC 19795-1 describes estimation methods for FAR and FRR indirectly through the estimation of the confidence interval of FMR and FNMR only when a genuine or imposter transaction consists of a single attempt. The developer may apply the estimation method for FNMR defined in Annex B.3.2.1 to estimate the confidence interval of FRR and an estimation method for FMR defined in Annex B.3.2.3 to estimate the confidence interval of FAR, assuming a single attempt is same as a single transaction.

However, several problems in the estimation methods defined in ISO/IEC 19795-1 are pointed out in literature, for example Interval estimation. The developer may use alternative confidence interval estimation methods (e.g. Agresti-Coull interval) proposed in the alternate literature. However, the developer shall describe the detail of the selected alternative method and a rationale why the method is selected in the report.

- Final test result

  The following values shall be reported.

  If FAR and FRR is selected in FIA_MBV_EXT.1, the number of total genuine and imposter transactions, the number of transactions incorrectly accepted or denied, the estimation methods of confidence interval and the upper bound of confidence interval for FAR and FRR shall be reported.

  If FMR and FNMR is selected in FIA_MBV_EXT.1, the number of total genuine and imposter attempts, the number of attempts falsely declared match or not to match, the estimation methods of confidence interval and the upper bound of confidence interval for FMR and FNMR shall be reported.

8.3.2. Target application and influential factors

The performance report shall specify a target application modelled in the test, such as biometric verification in an indoor office environment with a habituated crew.

The performance report 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 to appropriate documents (e.g. ISO/IEC 19795-3) 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 ISO/IEC 19795-3. Any information that is useful in the context of the used biometric modality shall be considered by the developer to determine the factors.

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

a. Test subject demographics

    1. Age

       The age distribution ratio by the following age groups: [0-19], [20-34], [35-49], [50-64], [65-99].

    2. Gender

       Female/Male ratio

    3. Ethnicity

       The distribution ratio by the ethnic background of the participants.

       The breakdown can be by one of two measures: UN geographical regions or by a measure of ethnicity defined in the nation where testing has taken place. One of these categorizations must be used in the reporting of demographic information.

b. Posture and positioning

   Posture of test subject or positioning of the 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

8.3.3. Test subject selection

The 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 the demographics of test subjects follow the target application.

8.3.4. 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 a test subject prior to 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

   Methods for how to confirm the level of subject habituation prior to biometric data collection shall be reported. If the habituation was confirmed through training, the 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)

8.3.5. 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)

8.3.6. 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 the flow of genuine and imposter attempts or transactions 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. The 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 failed because of such excluded samples, the number of such failed transactions shall also be reported.

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 computer is used by the single user without any support. The same advice or remedial actions shall be given to all test subjects with the same conditions.

Chapter 9. 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.

9.1. Recommendations

9.1.1. Test scenario for 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 biometric verification in a different way.

Suppose the computer provides both a NBAF and a BAF and the user can use either factor to unlock the device. One user may try to unlock the device with the BAF until allowable maximum number of unsuccessful authentication attempts is exceeded. Another user may try to unlock the device with the BAF only three times and switch to the NBAF 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 biometric verification.

However, it is not possible to evaluate all these scenarios to measure the performance. The developer shall define one test scenario and describe it in the ST.

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

This means that if FAR and FRR are selected, the developer shall define that the genuine and imposter transaction is consists of 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 FIA_MBV_EXT.1 if the developer considers the specific test scenario to measure the performance at the system level.

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.

9.1.2. 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.

The quality of the template may have a significant impact on the biometric verification performance. This BIOSD assumes that the user is familiar with the computer's operation and enrols correctly following the AGD guidance provided by the developer. The test subject may make enough practice attempts to become familiar with the device operation before the final enrolment transaction.

9.1.3. 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 9.1.1, "Test scenario for biometric verification".

9.1.4. Maximum number of transactions per test subject

Only one transaction can be run by each test subject because the computer locks the biometric verification as required by the Base-PP after the certain number of attempts are failed.

9.1.5. Cross-comparison for FAR/FMR

The BIOSD allows full cross-comparison to estimate FAR/FMR because it is commonly agreed that the statistical loss of computing all possible cross-comparisons between test subjects is acceptable.

This BIOSD also allows cross-comparison of attempts/templates of ordered pairs if there is no explicit reason that this cross-comparison hinders the accuracy of the result of performance testing. Cross-comparison of attempts/templates of ordered pairs allows the comparison 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 pairs, this assumption can not be used. The type of verification algorithm used by the TOE is reported in the developer's performance report Section 8.3.1, "Overview of the performance testing".

This BIOSD 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).

9.2. Example - fingerprint verification

The developer defines that fingerprint verification consists of 5 attempts using both right index and thumb fingerprints to unlock the computer and specifies a FAR not exceeding 0.01% for the upper bound of 95% confidence and a FRR not exceeding 5% for the upper bound of 80% confidence in FIA_MBV_EXT.1.

As described in the previous Section, the genuine and imposter transaction consists of 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 developer applies rule of 3 in Annex B of ISO/IEC 19795-1. To run more than 30,000 imposter transactions, at least 174 test subjects shall be gathered (173 * 174 = 30,102) if cross-comparison of ordered pairs is allowed. If number of test subjects is 174, only 5 genuine transactions can fail to achieve a 5% FRR with 80% confidence (upper bound estimated by equation B.1, B.2 and B.9 when 5 transaction denied = 0.045 < 5%).

If the developer specifies a FMR not exceeding 0.01% for the upper bound of 95% confidence and a FNMR not exceeding 5% for the upper bound of 80% confidence 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 of ordered pairs is allowed. If number of test subjects is 78, the total number of genuine attempts is 78 * 5 = 390 and single attempt from each 14 test subjects can be failed to achieve a 5% FNMR with 80% confidence (upper bound estimated by equation B.3, B.4 and B.9 when single attempt from each 14 test subjects are not matched = 0.049 < 5 %).

Chapter 10. Developer’s quality assessment criteria report of biometric samples

The term “quality” is used in FIA_MBE_EXT.2 and FIA_MBV_EXT.2 and these SFRs require the TOE to use biometric samples of sufficient quality. However, the quality of a biometric sample is interpreted differently throughout literature. In general, quality is defined as an indicator of the usefulness of the biometric sample for biometric enrolment and verification. The TOE can use this indicator to improve the TOE’s performance, especially FRR and FNMR, because the TOE can reject “bad” or low-quality samples at an early phase that would cause performance degradation.

The TOE uses quality assessment criteria to measure the indicator, namely, quality scores of samples measured by quality metrics and reject low-quality samples that fall below the quality threshold.

The BMD must provide an overview of the quality metrics and how such quality metrics are used so the evaluator can understand how the TOE meets FIA_MBE_EXT.2 and FIA_MBV_EXT.2; however, the BMD does not need to explain why the quality metrics can estimate the quality scores of samples. The developer shall conduct the testing to show the efficacy of quality metrics and report the result of testing in the quality assessment criteria report. This section defines the requirements for contents of report, referring to ISO/IEC 29794-1.

If the developer’s quality metrics conform to published standards and name of the standard (e.g. ISO/IEC 29794-4) is assigned in FIA_MBE_EXT.2 and FIA_MBV_EXT.2, the developer doesn’t need to test the efficacy of quality metrics because such efficacy had been verified by experts during the standardization process. However, the developer shall conduct the conformance test to show the implementations of TOE’s quality metrics conform with ones defined in the standard. For example, if the TOE implements the quality metrics for fingerprint defined in ISO/IEC 29794-4, the developer shall conduct the conformance test following the Annex A in ISO/IEC 29794-4 and quality scores measured by quality metrics implemented in the TOE from samples in the public databases specified in ISO/IEC 29794-4 shall not differ from ones measured by the reference implementation, as shown in Table A.1 of ISO/IEC 29794-4, by more than 1 % to claim the conformance. Requirements for the report are described in Section 10.1, “Requirements for the quality assessment criteria report (standard quality metrics)”.

The TOE may not conform to the standard quality metrics for various reasons, such as standards not existing for the modality that the TOE supports, or standard quality metrics need to be adjusted due to the limited computer resources. If the TOE doesn’t conform to a standard, *developer defined quality assessment method* shall be assigned in FIA_MBE_EXT.2 and FIA_MBV_EXT.2 and the developer shall conduct the test to show the efficacy of quality metrics implemented in the TOE. This means that the developer shall conduct the test to verify that those quality metrics serve as indicators of the usefulness of the biometric sample for biometric enrolment and verification and rejection of low-quality samples based on those metrics improves TOE’s performance. Requirements for the report are described in Section 10.2, “Requirements for the quality assessment criteria report (non-standard quality metrics)”.

10.1. Requirements for the quality assessment criteria report (standard quality metrics)

This Section defines required content of the quality assessment criteria report for the TOE that implements the standard quality metrics.

The report is most likely a separate confidential document and not part of the ST for public release.

10.1.1. Summary of contents

Table 3, "Quality Assessment Criteria Report Items (standard quality metrics)" shows items that shall be reported in the report. The name or structure of report does not need to follow Table 3, "Quality Assessment Criteria Report Items (standard quality metrics)". However, all items in Table 3, "Quality Assessment Criteria Report Items (standard quality metrics)" should be included somewhere in the report. If some items are not included in the report, the developer shall provide a rationale for such exclusion to the evaluator.

Table 3. Quality Assessment Criteria Report Items (standard quality metrics)

Section	Item
Section 10.1.3	Test configuration
Section 10.1.4	Quality metrics and expected scores
Section 10.1.5	Conformance test result
Section 10.1.6	Methods to create low-quality samples

10.1.2. Quality assessment criteria report (standard quality metrics)

This Section describes each item in Table 3, "Quality Assessment Criteria Report Items (standard quality metrics)" in detail. Most items are created based on the Section 8.3, "Reporting items description" so the developer may refer them to create the report.

The developer may point to a public standard used for the determining of quality metrics, such as ISO/IEC 29794-4 to provide the necessary information.

10.1.3. Test configuration

a. TOE Reference

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

   Modification to the TOE for testing, if any, shall be reported (e.g. the TOE is modified to export biometric data for reporting quality score). The rationale that such modification does not affect the TOE's quality control shall also be provided. For example, the developer may claim that the quality control is not affected because modified code is not executed during biometric verification or the developer may run regression tests to verify that modification does not change the result of the quality control (e.g. quality score).

b. TOE configuration

   Any configurable parameters or settings of the TOE that may affect the quality control shall be reported. The value of each parameter set for the testing shall also be provided. For example, if the threshold (e.g. sample quality threshold) is configurable by users, the value of the threshold set for the testing shall be reported.

c. Quality assessment test tools

   Information that uniquely identifies all testing tools (e.g. SDK) used for the quality assessment testing shall be reported.

10.1.4. Quality metrics and expected scores

a. Identification of standard quality metrics

   Quality metrics that the TOE implements shall be identified. For example, if the TOE implements the quality metrics in ISO/IEC 29794-4, name of the standard (ISO/IEC 29794-4:2017 Information technology — Biometric sample quality — Part 4: Finger image data) and name of quality metrics (e.g. Orientation certainty level in Section 5.2.2) that the TOE implements shall be identified.

b. Sample databases

   Sample databases used for the conformance test shall be reported. For example, ISO/IEC 29794-4 specifies the website where the database can be downloaded.

c. Expected quality scores (Expected test result)

   Quality scores that are measured by the reference implementation shall be reported. For example, ISO/IEC 29794-4 lists all quality scores from samples in the database for each quality metric.

d. Pass/Fail criteria

   Pass/Fail criteria shall be defined. For example, ISO/IEC 29794-4 states that no quality scores measured by TOE shall differ from expected ones by more than 1 % in order to conform the standard quality metrics.

10.1.5. Conformance test result

a. Test period

   Date of the conformance test shall be reported.

b. Actual quality scores (Actual test result)

   Quality scores of samples in the database that are measured by the TOE shall be reported.

c. Final conclusion

   The final conclusion of test based on Pass/Fail criteria shall be reported. If the TOE can't conform to the standard quality metrics, usefulness of TOE's quality metrics shall be tested and reported following Section 10.2, "Requirements for the quality assessment criteria report (non-standard quality metrics)".

10.1.6. Methods to create low-quality samples

Methods to create low-quality samples (e.g. varying temperature / humidity conditions of the finger skin, low physical pressure, too less presentation time or incorrect finger positioning angles for fingerprint verification) shall be described. This information is used for the evaluator to conduct the independent testing for FIA_MBE_EXT.2 and FIA_MBV_EXT.2.

10.2. Requirements for the quality assessment criteria report (non-standard quality metrics)

This Section defines required content of the quality assessment criteria report for the TOE that implements the non-standard quality metrics.

There are several test approaches to show the efficacy of quality metrics in literature and the followings are the popular ones that can evaluate the efficacy in quantifiable manner.

a. Correlation between the similarity score and quality score

   The quality score can be used as an indicator of the usefulness of the biometric sample if the quality score is strongly correlated with the similarity score. Based on such a quality score, the TOE can reject low-quality samples at the time of capture, reduce the false non-match and save the time for image processing such as segmentation and feature extraction for low-quality samples.

   Correlation can be computed using, for example, Spearman's rank correlation coefficient p that is a quantitative method to analyze how well two variables correlate. A value of 1 or -1 of p indicates being perfectly monotonically correlated, while 0 indicates being uncorrelated.

   The developer can compute the similarity score and quality score based on the TOE's quality metrics for collection of samples and compute the correlation to evaluate the efficacy of quality metrics.

   The detailed information of such test method is described in, for example, [Qualifying Fingerprint Samples].

b. Error Reject Curves

   Error reject curves (ERC) shows how efficiently rejection of low-quality samples can result in improved performance. If the TOE rejects low-quality samples whose quality scores are less than the quality threshold, and FNMR or FRR is improved because of this rejection, quality scores measured by TOE's quality metrics can work as an indicator of the usefulness of the biometric sample.

Thus, a good quality metric correctly labels those samples that cause low similarity scores as low-quality ones. For a good quality metrics, FNMR or FRR should decrease quickly with the fraction rejected.

The detailed information of ERC is described in, for example, [Performance of Biometric Quality].

c. Sample acceptance error tradeoff

The TOE needs to make decisions about whether or not to accept a sample for further processing based on quality metrics. Such decisions are subject to Type I/II error tradeoff analysis from decision theory. First, Type I errors express an incorrect rejection of a good biometric sample, i.e. assignment of low-quality when the sample would be enrolled or verified by the TOE correctly; and Type II errors express an incorrect acceptance of a low-quality sample when it ultimately gives a false negative.

Both error rates of the TOE's quality metrics should be low enough to serve as an indicator of the usefulness of the biometric sample for biometric enrolment and verification.

The detailed information of both Type I and II errors is described in, for example, [Ongoing Face Recognition Vendor Test].

The developer shall conduct the test following either of above approaches to show the efficacy of TOE's quality metrics and create the test report.

The report is most likely a separate confidential document and not part of the ST for public release.

10.2.1. Summary of contents

Table 4, "Quality Assessment Criteria Report Items (non-standard quality metrics)" shows items that shall be reported in the report. The name or structure of report does not need to follow Table 4, "Quality Assessment Criteria Report Items (non-standard quality metrics)". However, all items in Table 4, "Quality Assessment Criteria Report Items (non-standard quality metrics)" should be included somewhere in the report. If some items are not included in the report, the developer shall provide a rationale for such exclusion to the evaluator.

Table 4. Quality Assessment Criteria Report Items (non-standard quality metrics)

Section	Item
Section 10.1.3	Test configuration
Section 10.2.4	Quality metrics and expected test result
Section 10.2.5	Test result of TOE quality metrics
Section 10.1.6	Methods to create low-quality samples

10.2.2. Quality assessment criteria report (non-standard quality metrics)

This Section describes each item in Table 4, "Quality Assessment Criteria Report Items (non-standard quality metrics)" in detail. Most of items are created based on Section 8.3, "Reporting items description" so the developer may refer them to create the report.

10.2.3. Test configuration

Same as Section 10.1.3, “Test configuration”

10.2.4. Quality metrics and expected test result

a. Overview of TOE’s quality metrics

   The developer shall provide information for the TOE’s quality metrics in the BMD as described in the assessment strategy for FIA_MBE_EXT.2 and FIA_MBV_EXT.2. Such information is used to evaluate the CEM work units for ASE_TSS or AGD_OPE/ADV_FSP. Additional detail of TOE’s quality metrics shall be reported so that the evaluator can understand the result of test, if necessary.

b. Sample databases

   The developer shall use samples collected for the performance testing. If the developer adds samples to the database, the same procedure (e.g. Section 8.3.4, “Test instructions and training”) shall be applied for the addition of samples and the same level of information (e.g. Section 8.3.2, “Target application and influential factors”) for additional samples shall be reported.

c. Expected test result

   The developer shall conduct the test following either of the test methods described in Section 10.2, “Requirements for the quality assessment criteria report (non-standard quality metrics)”. Expected test results for each test are defined as follows.

   a. Correlation between the similarity score and quality score

      Correlation shall be measured by widely used method such as Spearman’s rank correlation coefficient and both scores shall show a clear correlation.

      Similarity score and quality score shall be categorized into 5 levels (lower levels indicate poorer sample properties). Most of samples in lowest level shall belong to the lowest level of the similarity score.

   b. Error Reject Curves

      ERC shall show that FNMR or FRR monotonically decreases as number of rejections of low-quality samples increases.

   c. Sample acceptance error tradeoff

      Both type I and type II error rates shall be less than 10%.

d. Pass/Fail criteria

   The evaluator shall make judgement whether or not the TOE’s quality metrics work as an indicator of the usefulness of the biometric sample for biometric enrolment and verification based on the test result.

10.2.5. Test result of TOE quality metrics

a. Test period

   Date of the test shall be reported.

b. Actual test result

   Correlation, ERC or Type I/II error of the TOE measured from the sample database shall be reported.

c. Final conclusion

   Final conclusion of the test based on Pass/Fail criteria shall be reported.

10.2.6. Methods to create low-quality samples

Same as Section 10.1.6, “Methods to create low-quality samples”

Chapter 11. Attack Potential and TOE resistance

11.1. Calculating attack potential for generic biometric system

Attack potential is a function of expertise, resources and motivation, as is written in [CEM]. The [CEM] provides general guidance for calculating attack potential for all type of IT products and this general guidance should be adjusted considering the specific characteristics of a particular type of IT products.

Currently, two ISO standards, ISO 19989 and ISO 25456 have tailored the guidance more specifically for biometrics. ISO 19989 and ISO 25456 define the framework for the PAD and biometric data injection attack detection evaluation respectively. There is similarity between both frameworks, however, there is a fundamental difference between the two.

ISO 19989 framework is conformant to the [CC] and [CEM] (This BIOSD is also conformant to the [CC] and [CEM] however, its scope is limited to AVA_VAN.1). Biometric product evaluations under ISO 19989 shall meet all requirements defined in ISO 19989, the [CC] and [CEM]. The level of AVA_VAN component that the TOE shall meet determines the level of resistance to attacks and evidence (e.g., design, configuration management or development lifecycle document) required for the evaluations.

On the other hand, ISO 25456 is not conformant to [CC] and [CEM] and doesn't use the AVA_VAN component. Instead, ISO 25456 reduces the number of requirements to enable the fixed-time evaluations and provides detail and specific guidance for the penetration testing.

However, both standards share almost the same attack potential table because the measure to gauge the level of presentation attack and biometric data injection attack should be consistent. Differences between the table in ISO 19989 and ISO 25456 are;

a. ISO 19989 adds a new level ⇐ *twelve hours* to **Elapsed Time** and *Opportunistic Easy (Enhanced-Easy)* to **Window of Opportunity (Access to Biometric Characteristics)** and defines higher values for **Window of Opportunity (Access to TOE)** in exploitation phase considering the nature of mobile devices.

b. Both standards define a few same factors with different name (e.g., **Elapsed Time** in ISO 19989 and **Time effort** in ISO 25456).

c. Guidance for factors in ISO 19989 is adjusted to the presentation attack and different from ones in ISO 25456.

This BIOSD defines the same attack potential table and guidance as defined in ISO 19989.

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

11.1.1. Identification and exploitation of attacks

11.1.1.1. 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.

11.1.1.2. 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.

Application Note 1

> For the evaluator, the work of the identification phase has to be fully performed: developing hardware and software, creating artefacts 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.

Application Note 2

> Exploitation consists of applying scripts, so it is expected that some factor values will be reduced from the identification phase, in particular "Elapsed Time" and "Expertise". These are accounted for in that the weighting for some factors during the exploitation phase are lower than the corresponding identification phase.

11.1.2. Factors to be considered

As in the [CEM], the factors to be considered consist of ***Elapsed time***, ***Expertise***, ***Knowledge of the TOE***, ***Equipment***, ***Window of opportunity*** and ***Degree of Scrutiny***. 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 an artefact 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)***).

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 an artefact in a known (published) way without specific difficulties (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 general knowledge of the attacks. An attacker of this level is capable of adapting known attack methods to their needs without needing deep expertise. 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 artefact 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 along with knowledge of state-of-the-art attacks. An attacker of this level is capable of generating their 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.

Application Note 3

> 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.

Application Note 4

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

Knowledge of the TOE refers to the amount of knowledge of the 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* information is considered public if it can be easily obtained by anyone (from internet for instance) or if it is provided by the developer to any customer without further means. It is important to consider that some public information may not be easily used, such as open source projects, where the code is available for anyone, but may require expertise or time to be of use.
b. *Restricted information* which is only shared by the developer and organizations which are using the system, usually under a non-disclosure agreement.
c. *Sensitive 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 rarely used for the exploitation phase and should be justified by the evaluator when using it.

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. The equipment is so specialized that its distribution is controlled, or the use of equipment requires either significant experience to master its operation or a human operator is hired together with the equipment; for example, high-grade printing systems with a human operator hired together. In addition, if more than one specialized equipment is required to perform different parts of the attack, this value should be used. Before using this level, the possibility of renting equipment should be determined. If such a service exists, the level shall be moved down to the specialized level.

Multiple Bespoke refers to needing different types of bespoke equipment, not a single system, for distinct steps in the attack.

Not practical refers to equipment that is too expensive or too difficult to obtain compared to any gains that may be made by an attacker.

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 enroled 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 except for cases that use synthetic images, and the rating only concerns the creation and the presentation of an artefact.

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 an artefact 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. *Not needed* is for attacks that do not need real biometric data to be available, for example, attacks based on synthetic images or template generation.

b. *Without notice (Easy)* is for making an artefact with samples that can be collected without any contact with an enroled subject. For example, 2D face images uploaded on the Internet and latent fingerprint images on a glass can be collected without notice of the subject.

c. *Opportunistic Easy (Enhanced-Easy)* is for making an artefact with samples that can be collected without any contact with an enroled subject, but for which the identity of the subject is not known prior to the attack, as in a target of opportunity vs a planned attack. In this case, while the necessary images may not be difficult to acquire, they may have to be acquired after the attack has started instead of beforehand.

d. *Non-cooperative (Moderate)* is for making an artefact with samples that need to be collected directly from an enroled subject in a short period of time without conscious cooperation from the subject. For example, iris or vein images need to be acquired with a high resolution or infrared camera, however, such images can be taken in a moment without conscious control of the subject.

e. *Cooperative (Difficult)* is for making an artefact with samples that need to be collected directly from an enroled subject with full cooperation from the subject. For example, the acquisition of a detailed 3D face scan of the subject takes time and requires full cooperation from the subject.

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 as known/unknown tuning) and organizational measures (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 are constraints such as having to steal the device where the owner of the system would become aware of the missing device within some defined time period.

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 artefacts must be adapted to the (unknown) specific tuning, or the system needs physical modification (for example physically accessing a hidden signal significant to the comparison score).

Degree of Scrutiny refers to the amount of examination or oversight applied during the use of the TOE for authentication.

The levels are as follows:

a. *None*: For the attack, there is no supervision during the attack attempt.

b. *Overseen*: For both the attack and discovery, there is a security agent or operator trained for fraud detection overseeing the use of the TOE. This oversight is limited for efficiency and may be remote as opposed to physically close.

c. *Not practical*: For both the attack and discovery there is a security agent physically present and close to the attacker with thorough control over the TOE during usage.

Application Note 5

An attack is considered not practical when an attacker is not confident enough to perform an attack, even when an exploit has been found.

11.1.3. Calculation of attack potential

Table 5, “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 5. Calculation of attack potential for general biometric system

Factor	Value	
	Identification	Exploitation
Elapsed Time		
⇐ one hour	0	0

Factor	Value	
⇐ twelve hours	0	1
⇐ one day	1	3
⇐ three days	2	4
⇐ one week (seven days)	3	6
⇐ 25 days	6	8
> 25 days	10	10
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple experts	7	6
Knowledge of TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Equipment		
Standard	0	0
Specialised	2	4
Bespoke	4	6
Multiple Bespoke	6	10
Not practical	*	*
Window of Opportunity (Access to Biometric Characteristics)		
Not needed	0	0
Without notice (Easy)	0	0
Opportunistic Easy (Enhanced-Easy)	0	2
Non-cooperative (Moderate)	4	4
Cooperative (Difficult)	8	8
Window of Opportunity (Access to TOE)		
Easy	0	0
Moderate	2	4
Difficult	4	8

Factor	Value	
Degree of Scrutiny		
None	0	0
Overseen	2	3
Not practical	*	*

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. However, Table 5 is intended as a guide. Evaluator may modify the table with a proper justification.

11.1.4. Rating of vulnerabilities and TOE resistance

The "Values" column of Table 6, “Rating of vulnerabilities and TOE resistance” indicates the range of attack potential values (calculated using Table 5, “Calculation of attack potential for general biometric system”) of an attack scenario that results in the SFRs being undermined.

Table 6. 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:
0-9	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

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
⇒40	Beyond-High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-
At least one "Not Practical" Mark	Not practical	Not practical	Not practical	

11.2. Application notes for BIOPP-Module

The attack potential table Table 5, “Calculation of attack potential for general biometric system” defined in previous Section does not 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 the 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_MBE_EXT.3 and FIA_MBV_EXT.3.

11.2.1. Application note for Elapsed time for Identification

The evaluator should select one week at maximum because the evaluator should finish the penetration testing within one week for the testing of a single biometric sensor. This is not intended to force the evaluator to spend a week of time for testing each sensor type when multiple sensor types are tested in a single evaluation. The evaluator shall provide a sufficient justification that the time taken in testing for each sensor type is equivalent to a week for a single sensor test (when only a single sensor would be tested in isolation).

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

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

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

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

11.2.4. Application note for Degree of Scrutiny for Identification and Exploitation

The evaluator shall select "None" because potential difficulties to having access to the TOE are taken into account in the factor ***Window of opportunity (Access to the TOE)*** for mobile devices.

Chapter 12. Related Documents

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2022-11-001, CC:2022 Revision 1, November 2022.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2022-11-002, CC:2022 Revision 1, November 2022.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2022-11-003, CC:2022 Revision 1, November 2022.
- [CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022 Revision 1, November 2022.
- [CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022 Revision 1, November 2022.
- [CEM] Common Methodology for Information Technology Security Evaluation, CCMB-2022-11-006, CC:2022 Revision 1, November 2022.
- [CC-E&I] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), 002, Version 1.1, July 22, 2024.
- [PP_MDF] Protection Profile for Mobile Device Fundamentals, September 12, 2022, Version 3.3.
- [CFG-MDF-BIO] PP-Configuration for Protection Profile for Mobile Device Fundamentals and collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [CFG-MDF-BIO], February 28, 2025, Version 2.0.
- [BIOPP-Module] collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], February 28, 2025, Version 2.0.
- [Toolbox] Toolbox Overview, October 15, 2024, Version 1.2.
- [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 revision.
- [ISO/IEC 25456] Biometrics — Biometric data injection attack detection, Under development.
- [ISO/IEC 29794-1] Information technology — Biometric sample quality - Part 1: Framework, First edition.
- [ISO/IEC 29794-4] Information technology — Biometric sample quality - Part 4: Finger image data, First edition.
- [ISO/IEC 30107-3] Biometric presentation attack detection - Part 3: Testing and reporting, First edition.
- [ISO/IEC 30107-4] Biometric presentation attach detection - Part 4: Profile for testing of mobile

devices, First edition.

- [Qualifying Fingerprint Samples] Qualifying Fingerprint Samples Captured by Smartphone Cameras in Real-Life Scenarios - May 3, 2016, http://hdl.handle.net/11250/2388306.
- [Performance of Biometric Quality] Performance of Biometric Quality Measures - April 16, 2007, https://www.nist.gov/publications/performance-biometric-quality-measures.
- [Ongoing Face Recognition Vendor Test] Ongoing Face Recognition Vendor Test (FRVT) Part 5: Face Image Quality Assessment - August 11, 2021, https://pages.nist.gov/frvt/reports/quality/frvt_quality_report.pdf.
- [Biometric quality] Biometric quality: a review of fingerprint, iris, and face - July 2, 2014, https://link.springer.com/article/10.1186/1687-5281-2014-34.
- [Vascular quality] State of the Art in Vascular Biometrics (1.6 Presentation Attacks and Detection, and Sample Quality) - November 14, 2019, https://link.springer.com/chapter/10.1007/978-3-030-27731-4_1#Sec21.