INTERNATIONAL STANDARD

ISO/IEC 19989-1

First edition
2020-09

Information security — Criteria and methodology for security evaluation of biometric systems —

Part 1: Framework

Sécurité de l'information — Critères et méthodologie pour l'évaluation de la sécurité des systèmes biométriques —

Partie 1: Cadre

Reference number
ISO/IEC 19989-1:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 19989 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Biometric systems can be vulnerable to presentation attacks where attackers attempt to subvert the system security policy by presenting their natural biometric characteristics or artefacts holding copied or faked characteristics. Presentation attacks can occur during enrolment or identification/verification events. Techniques designed to detect presentation artefacts are generally different from those to counter attacks where natural characteristics are used. Defence against presentation attacks with natural characteristics typically relies on the ability of a biometric system to discriminate between genuine enrolees and attackers based on the differences between their natural biometric characteristics. This ability is characterized by the biometric recognition performance of the system. Biometric recognition performance and presentation attack detection have a bearing on the security of biometric systems. Hence, the evaluation of these aspects of performance from a security viewpoint will become important considerations for the procurement of biometric products and systems.

Biometric products and systems share many of the properties of other IT products and systems which are amenable to security evaluation using the ISO/IEC 15408 series and ISO/IEC 18045 in the standard way. However, biometric systems embody certain functionality that needs specialized evaluation criteria and methodology which is not addressed by the ISO/IEC 15408 series and ISO/IEC 18045. Mainly these relate to the evaluation of biometric recognition and presentation attack detection. These are the functions addressed in the ISO/IEC 19989 series.

ISO/IEC 19792 describes these biometric-specific aspects and specifies principles to be considered during the security evaluation of biometric systems. However, it does not specify the concrete criteria and methodology that are needed for security evaluation based on the ISO/IEC 15408 series.

The ISO/IEC 19989 series provides a bridge between the evaluation principles for biometric products and systems defined in ISO/IEC 19792 and the criteria and methodology requirements for security evaluation based on the ISO/IEC 15408 series. The ISO/IEC 19989 series supplements the ISO/IEC 15408 series and ISO/IEC 18045 by providing extended security functional components together with supplementary activities related to these requirements. The extensions to the requirements and supplementary activities found in the ISO/IEC 15408 series and ISO/IEC 18045 relate to the evaluation of biometric recognition and presentation attack detection which are particular to biometric systems.

This document consists of the introduction of the general framework for the security evaluation of biometric systems, including extended security functional components, and supplementary methodology and evaluation activities for the evaluator. The detailed recommendations are developed for biometric recognition aspects in ISO/IEC 19989-2 and for presentation attack detection aspects in ISO/IEC 19989-3.

In this document, the term "user" is used to mean the term "capture subject" used in biometrics.

Information security — Criteria and methodology for security evaluation of biometric systems —

Part 1: Framework

1 Scope

For security evaluation of biometric recognition performance and presentation attack detection for biometric verification systems and biometric identification systemsthis document specifies:

- extended security functional components to SFR Classes in ISO/IEC 15408-2;
- supplementary activities to methodology specified in ISO/IEC 18045 for SAR Classes of ISO/IEC 15408-3.

This document introduces the general framework for the security evaluation of biometric systems, including extended security functional components, and supplementary activities to methodology, which is additional evaluation activities and guidance/recommendations for an evaluator to handle those activities. The supplementary evaluation activities are developed in this document while the detailed recommendations are developed in ISO/IEC 19989-2 (for biometric recognition aspects) and in ISO/IEC 19989-3 (for presentation attack detection aspects). This document is applicable only to TOEs for single biometric characteristic type. However, the selection of a characteristic from multiple characteristics in SFRs is allowed.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382:2008, *Information technology — Vocabulary*

ISO/IEC 2382-37:2017, *Information technology — Vocabulary— Part 37: Biometrics*

ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance*

ISO/IEC 18045:2008, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382:2008, ISO/IEC 2382-37:2017, ISO/IEC 15408-1:2009, ISO/IEC 18045:2008, and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
attack presentation classification error rate
APCER
proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario

[SOURCE: ISO/IEC 30107-3:2017, 3.2.1]

3.2
attack type
element and characteristic of a presentation attack, including PAI species, concealer or impostor attack, degree of supervision, and method of interaction with the capture device

[SOURCE: ISO/IEC 30107-3:2017, 3.1.3]

3.3
bona fide presentation
interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system

Note 1 to entry: Bona fide is analogous to normal or routine, when referring to a bona fide presentation.

Note 2 to entry: Bona fide presentations can include those in which the user has a low level of training or skill. Bona fide presentations encompass the totality of good-faith presentations to a biometric data capture subsystem.

[SOURCE: ISO/IEC 30107-3:2017, 3.1.2]

3.4
bona fide presentation classification error rate
BPCER
proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

[SOURCE: ISO/IEC 30107-3:2017, 3.2.2]

3.5
PAI species
class of presentation attack instruments created using a common production method and based on different biometric characteristics

EXAMPLE 1 A set of fake fingerprints all made in the same way with the same materials but with different friction ridge patterns would constitute a PAI species.

EXAMPLE 2 A specific type of alteration made to the fingerprints of several data capture subjects would constitute a PAI species.

Note 1 to entry: The term “recipe” is often used to refer to how to make a PAI species.

Note 2 to entry: Presentation attack instruments of the same species may have different success rates due to variability in the production process.

[SOURCE: ISO/IEC 30107-3:2017, 3.1.6]

3.6
penetration testing
testing used in vulnerability analysis for vulnerability assessment, trying to defeat vulnerabilities of the TOE based on the information about the TOE gathered during the relevant evaluation activities

Note 1 to entry: In the ISO/IEC 15408 series, this term is used without definition.

3.7
presentation attack
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: Presentation attack can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc.

Note 2 to entry: Presentation attacks may have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: Biometric systems may not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations.

[SOURCE: ISO/IEC 30107-1:2016, 3.5]

3.8
presentation attack detection
PAD
automated determination of a presentation attack

Note 1 to entry: PAD cannot infer the subject's intent. In fact it may be impossible to derive that difference from the data capture process or acquired sample.

[SOURCE: ISO/IEC 30107-1:2016, 3.6]

3.9
presentation attack instrument
PAI
biometric characteristic or object used in a presentation attack

Note 1 to entry: The set of PAI includes artefacts but would also include lifeless biometric characteristics (i.e. stemming from dead bodies) or altered biometric characteristics (e.g. altered fingerprints) that are used in an attack.

[SOURCE: ISO/IEC 30107-1:2016, 3.7]

Note 2 to entry: Examples of altered biometric characteristics are mutilation, surgical switching of fingerprints between hands and/or toes (See Table 1 in 5.2 of ISO/IEC 30107-1:2016).

4 Symbols and abbreviated terms

APCER	attack presentation classification error rate
BPCER	bona fide presentation classification error rate
IT	information technology
FAR	false acceptance rate
FAU	SFR class of audit

NOTE The class name is defined in ISO/IEC 15408-2. Here, F of FAU stands for functional requirement, AU for audit. The class name is defined in this way in the ISO/IEC 15408 series. For details, see Annex A.

FMR	false match rate
FNIR	false-negative identification-error rate
FNMR	false non-match rate
FPIR	false-positive identification-error rate
FPT	SFR class of protection of the TSF
	NOTE See NOTE to FAU.
FRR	false rejection rate
FTAR	failure-to-acquire rate
FTER	failure-to-enrol rate
PAD	presentation attack detection
PAI	presentation attack instrument
PP	protection profile
SAR	security assurance requirement
SFR	security functional requirement
ST	security target
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface

5 General remarks

In addition to the requirements and recommendations provided in Clause 7 and Clause 8, those in ISO/IEC 15408-2 shall be applied.

In addition to the requirements and recommendations provided in Clause 9 to Clause 15, those in ISO/IEC 15408-3 and ISO/IEC 18045 shall be applied.

Annex D provides background information on supplementary activities for PAD evaluation.

The definition of authentication can be found in ISO/IEC 2382.

The definitions of biometric (adjective), biometric capture, assurance, biometric capture device, biometric characteristic, biometric concealer, biometric enrolee, biometric enrolment, biometric enrolment database, biometric feature, biometric identification, biometric impostor, biometric presentation, biometric recognition, biometrics, biometric reference, biometric sample, biometric system, biometric verification, comparison, enrol, failure-to-acquire rate, failure-to-enrol rate, alse match rate, false-negative identification-error rate, false non-match rate, false-positive identification-error rate, identify, match (noun) and threshold (noun) can be found in ISO/IEC 2382-37.

NOTE 1 In this document, the expression "capture device" is sometimes used instead of "biometric capture device".

NOTE 2 In this document, the expression "concealer" is sometimes used instead of "biometric concealer".

NOTE 3 In this document, the expression "impostor" is sometimes used instead of "biometric impostor".

The definitions of administrator, assignment, assurance, attack potential, class, component, confirm, delivery, describe, determine, developer, development, element, ensure, evaluation, extension, family, guidance documentation, identity, interaction, interface, life-cycle, object, operation ⟨on a component of ISO/IEC 15408⟩, operation, operational environment, potential vulnerability, Protection Profile, Protection Profile evaluation, security requirement, Security Target, ST evaluation, subject, target of evaluation, TOE security functionality, TSF data, TSF interface, TSF self-protection, verify and vulnerability can be found in ISO/IEC 15408-1.

NOTE 4 The second "operation" is related to the AGD class.

The definitions of action, activity, check, examine, methodology, report, scheme, sub-activity and work unit can be found in ISO/IEC 18045.

6 Vulnerabilities in biometric systems and security evaluation

6.1 Categorization of common vulnerabilities of biometric systems

In ISO/IEC 19792:2009, 8.3, common vulnerabilities of biometric systems are categorized into the following ten factors:

a) performance limitations;

b) artefact of biometric characteristics;

c) modification of biometric characteristics;

d) difficulty of concealing biometric characteristics;

e) similarity due to blood relationship;

f) special biometric characteristics;

g) synthesized wolf biometric samples;

h) hostile environment;

i) procedural vulnerabilities around the enrolment process; and

j) leakage and alteration of biometric data.

NOTE 1 All of the factors listed above are not vulnerabilities of biometric systems but each is related to them. In this document, the vulnerabilities of the factors or those related to factors, and their relations to security evaluation are considered.

Figure 1 shows the relationship between the vulnerability factors described in ISO/IEC 19792 and the types of evaluation described in this document.

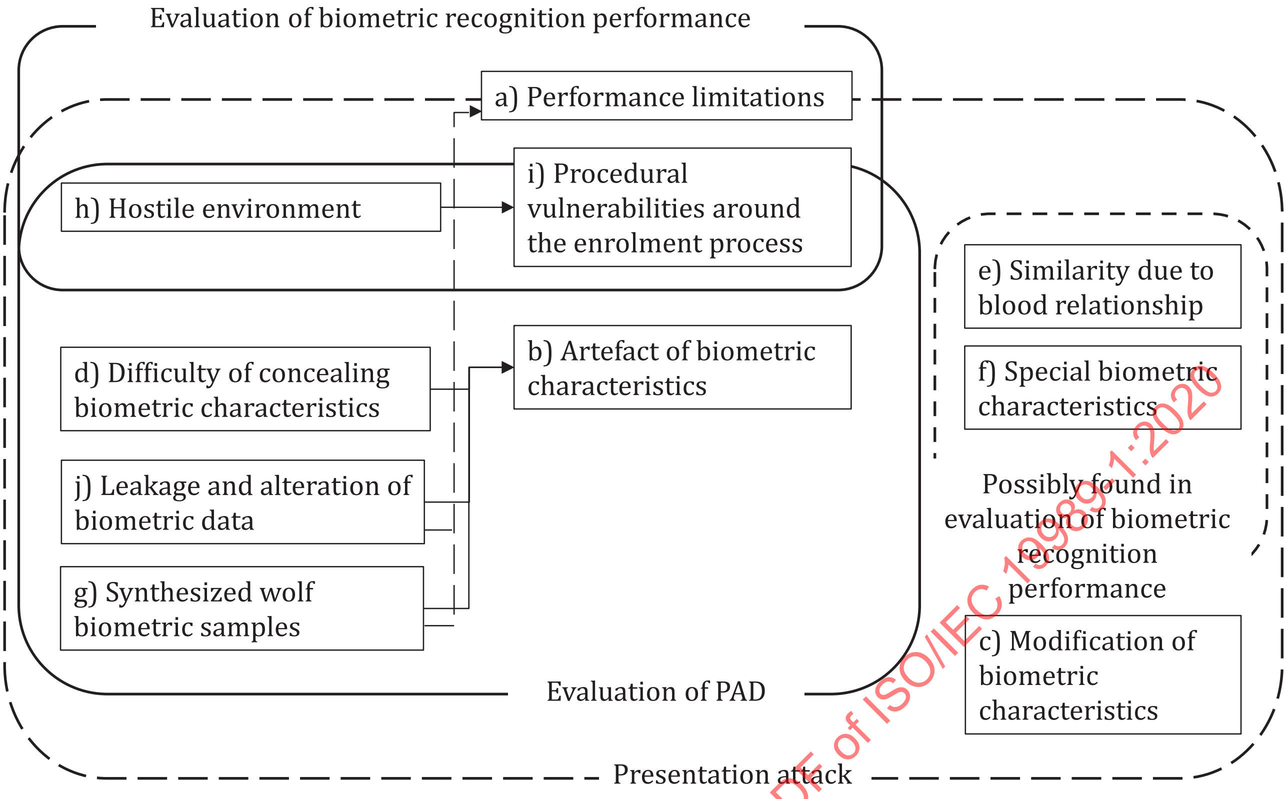
Evaluation of biometric recognition performance
a) Performance limitations
h) Hostile environment
i) Procedural vulnerabilities around the enrolment process
e) Similarity due to blood relationship
f) Special biometric characteristics
d) Difficulty of concealing biometric characteristics
b) Artefact of biometric characteristics
j) Leakage and alteration of biometric data
Possibly found in evaluation of biometric recognition performance
g) Synthesized wolf biometric samples
c) Modification of biometric characteristics
Evaluation of PAD
Presentation attack

Figure 1 — The relation of vulnerability factors in biometric systems

Factor j) is important as related to the protection of TSF-data/used data (see ISO/IEC 19792). In this document, however, factor j) is considered only from the standpoint of its exploitation by attackers to facilitate the construction of PAIs or mounting attacks related to biometric recognition performance. The evaluation of measures to protect biometric data from leakage or alteration is not addressed here.

Factor a), inherent in all biometric systems, can lead to false acceptances and false rejections, and is addressed in the biometric recognition performance evaluation. However, it can be also considered in relation to the zero-effort attack (presentation from impostor attempts under the policy of the intended use following the TOE guidance documentation). Thus, the biometric recognition performance evaluation and the PAD evaluation interrelate to each other. This factor is relevant to enrolment, verification, and identification.

Other factors are relevant to presentation attacks. However, factors e) and f) are out of scope for a PAD evaluation. Factor f) relates to individuals who have unusual natural biometric characteristics that make them more than usually liable to generate an apparent match against those of other people. However, such individuals are likely to be very difficult to find for the purpose of testing during an evaluation. They can be accidentally found as the result of the evaluation of biometric recognition performance. For factor e), it is difficult to collect such samples for the security evaluation. Outlier subjects giving rise to abnormally high biometric recognition performance can be encountered during biometric recognition performance testing. This can reveal a potential vulnerability in the TOE and relevant information should be used to inform the AVA evaluation activity.

Factor c) may be seen as a means of presentation attack that would exploit recognition weaknesses such as those revealed with a) and f) but thus to be considered in the vulnerability analysis phase. However, it requires extra elements beyond the scope of the objective evaluation. For example, surgery to embed the biometric characteristic of another person requires a sacrifice by the test subject and mimicry requires special skills to be developed by them.

Therefore, factors b), d), g), h), and i) are the factors to be evaluated in ISO/IEC 15408 evaluation for PAD. Factor i) needs to be considered only in enrolment. Factors b), g), and h) are relevant to enrolment, verification, and identification, but note that factor i) is influenced by factor h) as described in ISO/IEC 19792. A hostile environment can cause an enrolment of poor-quality biometric references that can later be compared to similarly poor quality biometric samples (see ISO/IEC 19792:2009, 8.3.9 and 8.3.10 for further information). Note that factors h) and i) are to be evaluated in ISO/IEC 15408 evaluation for biometric recognition performance. Factor d) refers to the fact that many biometric characteristics are not hidden and Hence, are potentially vulnerable to capture and recording for use in the construction of PAIs to make presentation attacks (e.g. latent fingerprint images, photographs of faces, recordings of voices). Hence, it shall be taken into account when calculating the attack potential of an attack (see F.1). Factor g) should also be considered in biometric recognition performance evaluation, as wolf samples can be exploited by an attack on the system elsewhere than on the data capture subsystem (e.g. via logical injection of a sample during the recognition process). This is related to the vulnerability analysis tasks in ISO/IEC 19989-2.

NOTE 2 Factor g) is indirectly related to factor f). Factor f) can be regarded as a naturally occurring variant of factor g) so that evaluation of the resistance of a TOE to synthesied wolf samples can provide an insight into the potential vulnerability to naturally occurring special biometric characteristics.

An attacker can have a variety of objectives: A biometric impostor would try to be recognized as a biometric enrolee other than themselves. A biometric concealer would try to avoid being matched to their own biometric reference.

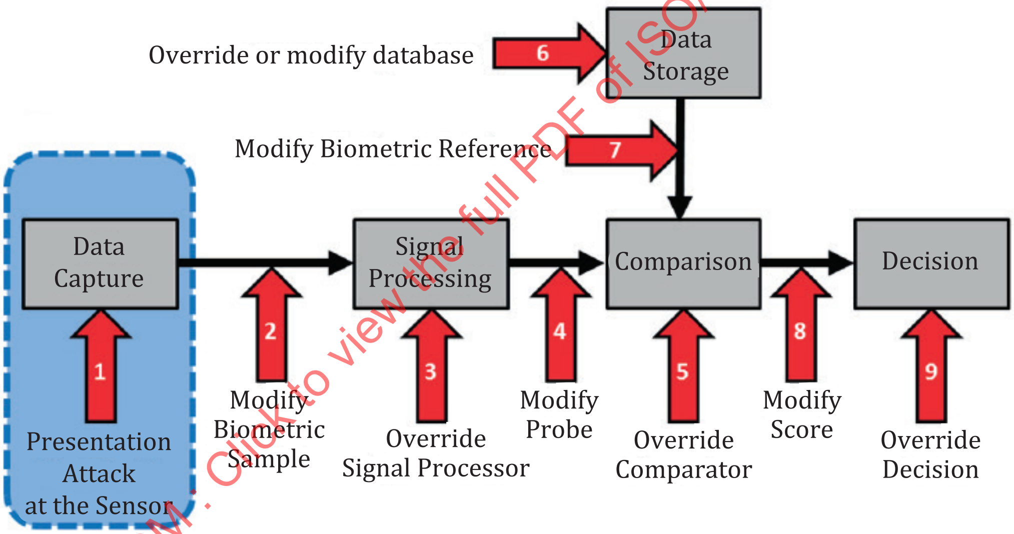

Figure 2 — Examples of points of attack in a biometric system (from ISO/IEC 30107-1)

Figure 2 illustrates generic attacks against a biometric system. Among these attacks, the attack indicated with arrow 1 is a presentation attack and those indicated with arrows 2 and 4 mark places where attacks can be made against captured biometric sample data and relate to biometric recognition performance. Points of attack 2 and 4 are considered in ISO/IEC 19989-2 only when the attack scenario is related to exploiting specific behaviour of biometric recognition performance (for example algorithm weaknesses). The other aspects are covered by generic IT security evaluation approaches and are not specific to the security evaluation of a biometric system. As a summary, the objectives of ISO/IEC 19989-2 and ISO/IEC 19989-3 are the following.

For ATE, ISO/IEC 19989-2 deals with the testing of biometric recognition performance in order to evaluate presentations from impostor attempts under the policy of the intended use following the TOE guidance documentation.

ISO/IEC 19989-3 deals with the testing of presentation attack detection mechanism.

For AVA, ISO/IEC 19989-2 is for all vulnerabilities that are biometric-specific (i.e. related to some extent to biometric recognition performances), excluding those with presentation at the capture subsystem against the policy of the intended use following the TOE guidance documentation; ISO/IEC 19989-3 is related to any vulnerability with a presentation attack at the capture subsystem which is made against the policy of the intended use following the TOE guidance documentation.

NOTE 3 Vulnerabilities possibly combined with IT vulnerabilities to those above mentioned are also in scope of security evaluation based on ISO/IEC 15408.

6.2 Biometric system and presentation attack detection

A common purpose of a biometric system is to recognize individuals by means of their biometric characteristics. A data subject presents one or more biometric characteristics to a biometric capture device of the biometric system for enrolment, verification, or identification. During the capture process, biometric samples are acquired from which the biometric features are extracted. At the enrolment stage, the extracted biometric features are used to create a biometric reference that is stored in the enrolment database. At the verification/identification stage, the biometric features are used to create a biometric sample for comparison against the relevant biometric reference(s). Figure 3 is a conceptual representation of a biometric system containing a PAD subsystem. The PAD subsystem functionality is typically not implemented as a distinct subsystem as indicated in Figure 3 but is incorporated within the one or more subsystems comprising the biometric system (e.g. data capture subsystem, signal processing subsystem).

Figure 3 is a conceptual representation of a biometric system containing a PAD subsystem. The PAD subsystem mechanism is typically not implemented as a distinct subsystem as indicated in Figure 3 but is incorporated within the one or more subsystems comprising the biometric system (e.g. data capture subsystem, signal processing subsystem). A presentation attack can be performed by presenting a presentation attack instrument (e.g. an an artificial object and others used in the attack) to a biometric system. The PAD subsystem is used at the verification/identification stage and also at the enrolment stage.

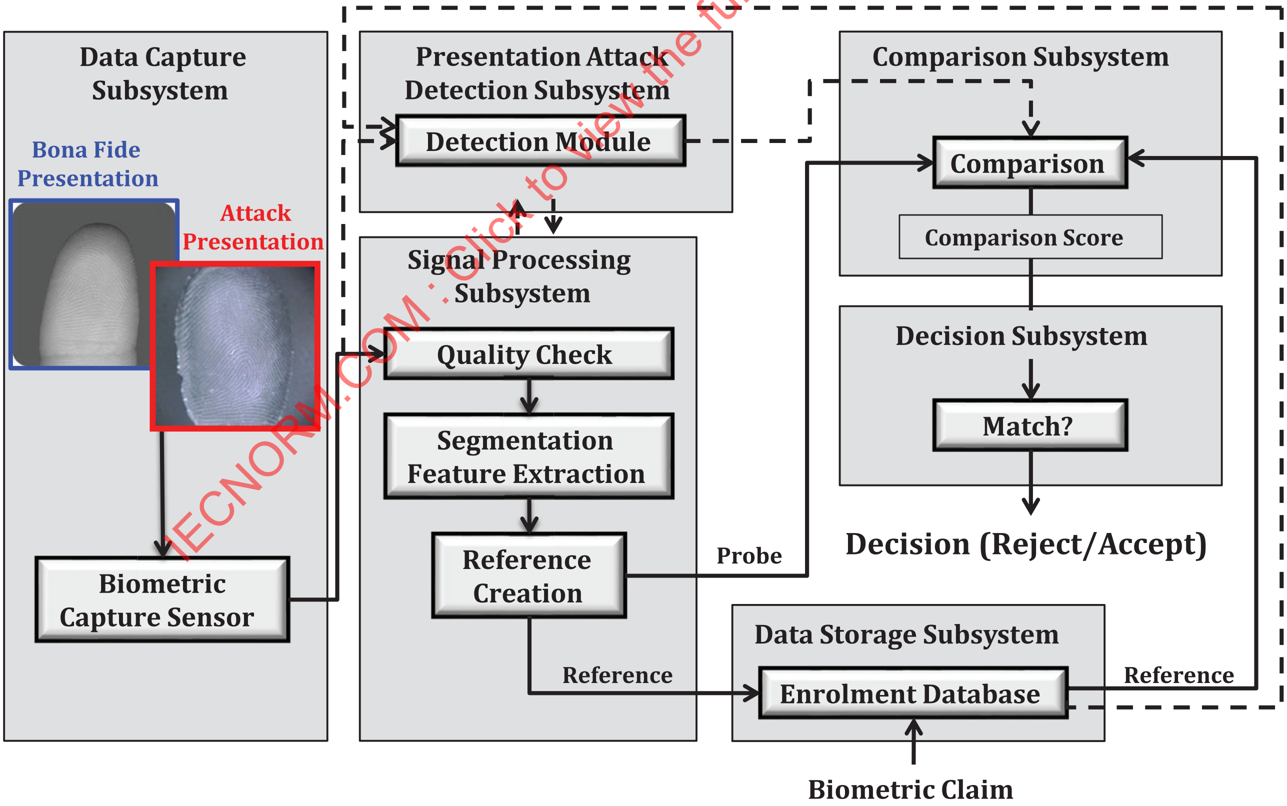

Figure 3 — General biometric framework incorporating PAD subsystem (conceptual representation)

NOTE Figure 3 is taken from ISO/IEC 30107-1 and modified replacing an old term with bona fide presentation. A dashed line in Figure 3 shows an interaction between the PAD subsystem and another subsystem. "Biometric Claim" in Figure 3 means claim of biometric reference.

Figure 4, also taken from ISO/IEC 30107-1, provides additional details of the PAD subsystem which is explained in ISO/IEC 30107-1:2016, 6.4.1, as follows:"Some PAD subsystems may not need the PAD feature extractor. The PAD comparator and the stored PAD criteria are essential in the subsystems".

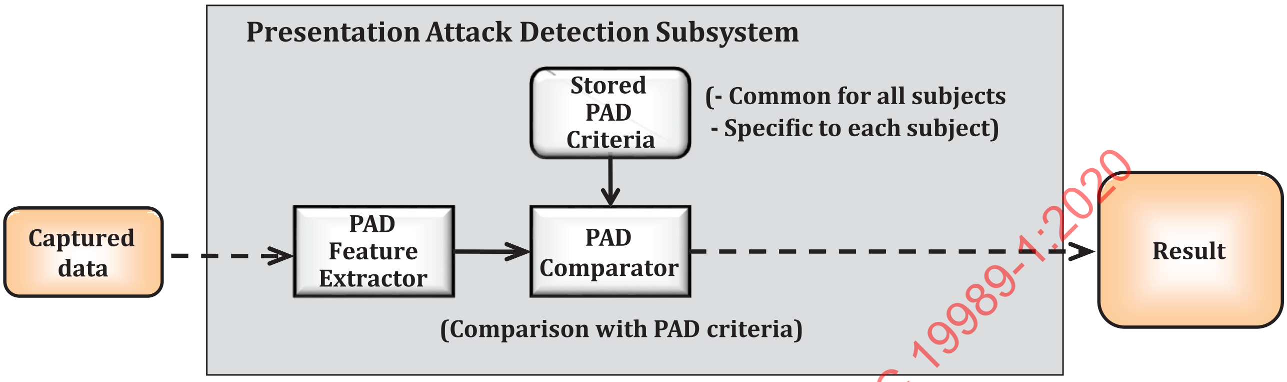
Presentation Attack Detection Subsystem
Stored PAD Criteria
(- Common for all subjects
- Specific to each subject)
Captured data
PAD Feature Extractor
PAD Comparator
Result
(Comparison with PAD criteria)

Figure 4 — Components in a general PAD subsystem

ISO/IEC 30107-1:2016, 6.4.2, describes the relationship between the PAD subsystem and the other biometric subsystems as follows:

"It is instructive to consider the collection and processing of the PAD data and the biometric sample data independently in both time and space. The two forms of data may both exist or either can exist in the absence of the other. The process of PAD can be handled by a biometric system concurrently, before, or after any of the subsystems. The components of the PAD subsystem may even occur separately, between and/or concurrently with more than one subsystem. PAD output may depend on multiple captured biometric samples and is not necessarily a simple binary indicator".

PAD techniques can include hardware sensing of presentation attacks and analysis of biometric sample and other relevant data looking for suspicious conditions or activity. Multiple techniques may be employed with decisions based on the fusing of results from each technique.

When evaluating a PAD mechanism all security relevant hardware and software components shall be considered, including the components that are involved in the process of gathering presentation evidence. In some cases, the normal capture sensor used in the biometric subsystem can provide this information. In other cases, a dedicated capture sensor for PAD may be employed. If the capture of the recognition sample and the capture of the presentation evidence are separated in space or time, this can allow presentation attacks to target the two capture processes individually and thereby create a potential vulnerability. Such vulnerabilities need to be assessed during the evaluation process (see ISO/IEC 19989-3).

6.3 Categorization of TOEs in relation to the type of evaluation

6.3.1 Biometric recognition performance evaluation

In the context of biometic recognition performance evaluation, TOEs are classified into two categories. The first category is where the biometric recognition mechanism of the TOE comprises solely software mechanisms which may be distributed through multiple subsystems but do not contain a biometric capture device. In this category, the TOE contains the comparison subsystem at least and may contain other subsystem(s). The second category is that the TOE comprises a complete biometric system including the biometric capture subsystem (with a biometric capture device).

Biometric recognition performance testing shall be performed by a technical test of the biometric recognition algorithm using a previously obtained test database containing biometric samples and biometric references or alternatively by a scenario test together with a test crew who are enrolled with a given combination of other subsystems including the data capture subsystem. In the first category, only technology evaluation is possible. In the second category, it is very likely that biometric recognition performance testing is carried out in form of a scenario evaluation (according to ISO/IEC 19795-1) with a test crew while both evaluations are possible.

NOTE In both of the above categories the biometric recognition performance results relate to a complete system. In the first category, the TOE comprises only part of the complete system. In the second category, it comprises the complete system. In the first category, the complete system that comprises the TOE and the other subsystems that form the evaluation environment are described in the security target, and the evaluation results only apply for that environment.

The following list identifies a set of typical types of TOEs from the biometric world and gives some guidance about their special aspects that need consideration.

— Software only TOE: a software-only TOE comprises an algorithm for comparison only or feature extraction and comparison. This is of specified interest in cases of composed systems in which one developer only provides the algorithm. In such a case, it can be useful to evaluate the security characteristics of the algorithm under appropriate assumptions about its environment. Afterwards, the algorithm can be integrated into a wider system scope and a new evaluation of the complete system may reuse the results of the evaluation of the algorithm. Another field in which a pure software TOE can be desirable is the smartcard world. A comparison-on-card (or match-on-card) system for example would usually only comprise the software for comparison, which is intended to work only on a secure electronic chip.

— Complete system including a biometric capture device: A complete biometric system is defined as the TOE comprising all the relevant functionality and security characteristics.

The extended components of SFRs for biometric recognition performance are specified in Clause 8.

6.3.2 PAD evaluation

In the context of PAD evaluation, TOEs are classified into three cases. The first case is the one which only contains a PAD subsystem and does not provide other biometric recognition functionalities. The second case is the one which contains the data capture subsystem and quality check functionality addition to PAD mechanism but does not contain the comparison subsystem. The third case is the one which contains at least the comparison and decision subsystems for biometric verification or identification in addition to PAD mechanism. This can contain data capture subsystem or not. The biometric verification software on smartphone, which is not provided from a smartphone vendor, and an IC card providing on-card biometric comparison only, are examples of TOE of the third case which do not contain a data capture subsystem. When a PAI is rejected by a TOE in the latter two cases, the evaluator can or may not know whether the rejection was the result of detection by the PAD subsystem or for some other reason such as failure to acquire, poor sample quality, failure to match, timeout, etc., depending on the information provided by the TOE to the evaluator.

The SFRs to be applied depend on which case a TOE belongs to. If the TOE belongs to the first case of PAD subsystem, then the extended components of SFRs specified in 7.2 shall be applied. If the TOE belongs to the second case, then the extended components of SFRs specified in 7.3 shall be applied. Otherwise if the TOE belongs to the third case, then the extended components of SFRs specified in Clause 8 shall be applied.

7 Extended security functional components to Class FPT: Protection of the TSF

7.1 General

This clause provides the definition of the additional families FPT_PAD and FPT_BCP of Class FPT, specified in ISO/IEC 15408-2, which can be used in protection profiles and security targets in order to model the security mechanisms of PAD subsystem and data capture subsystem with PAD. FPT_BCP and FPT_BCP are families which are applied respectively to the first and the second case of TOEs given in 6.3.2.

Some of the following SFRs have assignments that allow an ST or PP author to specify the biometric characteristic that is used to implement the mechanism (e.g. a fingerprint). These assignments serve to facilitate the understanding of the reader of the final ST.

Annex B provides explanatory information for the extended security functional components to Class FPT and shall be consulted when using the components identified in Clause 7.

NOTE The Class FPT is a Class "Protection of the TSF" specified in ISO/IEC 15408-2 (see ISO/IEC 15408-2:2008, Clause 14, and also Annex A).

7.2 Presentation attack detection (FPT_PAD)

7.2.1 Family behaviour

This family defines security functional requirements to detect biometric presentation attacks.

NOTE FPT_PAD is a family for a TOE of the first category classified in 6.3.2.

7.2.2 Component levelling

Figure 5 shows the structure of this family.

FPT_PAD Presentation attack detection
1

Figure 5 — FPT_PAD presentation attack detection family

FPT_PAD.1 presentation attack detection, detects presentation attacks for biometrics meeting or exceeding the criteria specified to the TOE.

7.2.3 Management of FPT_PAD.1

The following action can be considered for the management functions in FMT: management of the parameters used for presentation attack detection.

7.2.4 Audit of FPT_PAD.1

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: presentation attack detected;

b) basic: bona fide presentation detected.

7.2.5 FPT_PAD.1 Presentation attack detection

Hierarchical to: No other components

Dependencies: FMT_MTD.3 secure TSF data

FMT_SMF.1 specification of management functions

FPT_PAD.1.1

The TSF shall be able to distinguish between bona-fide presentations and attack presentations.

FPT_PAD.1.2

If a presentation attack is detected, the following action(s) shall be performed: [assignment: *list of actions*].

FPT_PAD.1.3

If a bona fide presentation is detected, the following action(s) shall be performed: [assignment: *list of actions*].

FPT_PAD.1.4

Along with the feedback about presentation attack status, detected or not detected, the TSF shall deliver the following information: [assignment: *list of information*].

NOTE In ISO/IEC 15408-2, FPT_PAD.1.1, FPT_PAD.1.2, FPT_PAD.1.3, and FPT_PAD.1.4 would be numbered as 7.2.5.1, 7.2.5.2, 7.2.5.3, and 7.2.5.4, respectively.

7.3 Biometric capture with presentation attack detection (FPT_BCP)

7.3.1 Family behaviour

This family defines security functional requirements for biometric capture with presentation attack detection supported by the TSF. This family also defines the required attributes on which the biometric capture mechanisms with presentation attack detection must be based.

NOTE FPT_BCP is a family for a TOE of the second category classified in 6.3.2.

7.3.2 Component levelling

Figure 6 shows the structure of this family.

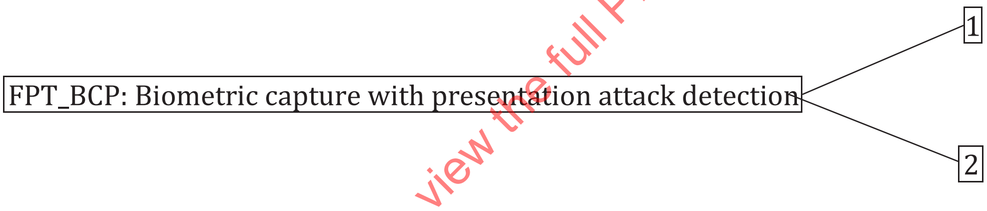
FPT_BCP: Biometric capture with presentation attack detection
1
2

Figure 6 — FPT_BCP Biometric capture with presentation attack detection family

FPT_BCP.1 check of biometric samples for biometric capture with presentation attack detection, requires the TSF to prevent generation of biometric samples or report the detection of presentation attack if presentation attack instruments are presented.

FPT_BCP.2 biometric capture with low failure rate, requires the TSF not to generate only biometric samples of extremely good quality in order to prevent from being used for enrolling only such biometric samples to achieve apparent good performance in biometric verification/identification afterwards, and also requires the TSF to limit FTAR within a specified rate.

7.3.3 Management of FPT_BCP.1

The following actions can be considered for the management functions in FMT:

a) the management of the TSF data, which include, for example, threshold values for quality scores to generate biometric sample by an administrator;

b) the management of the TSF data, which include, for example, values for detecting presentation attack instruments by an administrator.

7.3.4 Management of FPT_BCP.2

The following action can be considered for the management function in FMT: the management of the TSF data, which include, for example, threshold values for quality scores to generate biometric sample by an administrator.

7.3.5 Audit of FPT_BCP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) minimal: rejection by the TSF of data that is checked as low quality or detected as presentation attack instrument;

b) basic: rejection or acceptance by the TSF of data that is quality checked or input to biometric capture subsystem with presentation attack detection;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for quality scores and detecting presentation attack instruments.

NOTE The Class FAU is a Class "Security audit" specified in ISO/IEC 15408-2 (see ISO/IEC 15408-2:2008, Clause 14).

7.3.6 Audit of FPT_BCP.2

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: rejection by the TSF of data that is checked as low quality;

b) basic: rejection or acceptance by the TSF of data that is quality checked;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for quality scores of biometric data for capture.

7.3.7 FPT_BCP.1 Check of biometric samples for capture

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_BCP.1.1

The TSF shall prevent the use of non-artificial presentation attack instruments for generation of biometric samples from [assignment: *biometric characteristic*] that has been presented by any user of the TSF.

FPT_BCP.1.2

The TSF shall prevent the use of artificial presentation attack instruments for the generation of biometric samples from [assignment: *biometric characteristic*] that have been presented by any user of the TSF.

NOTE In ISO/IEC 15408-2, FPT_BCP.1.1 and FPT_BCP.1.2 would be numbered as 7.3.7.1 and 7.3.7.2, respectively.

7.3.8 FPT_BCP.2 Biometric capture with low failure rate

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_BCP.2.1

The TSF shall provide a mechanism to capture biometric data from [assignment: *biometric characteristic*] with the FTAR not exceeding [assignment: *defined value*].

NOTE In ISO/IEC 15408-2, FPT_BCP.2.1 would be numbered as 7.3.8.1.

8 Extended security functional components to Class FIA: Identification and authentication

8.1 General

This clause provides the definition of the additional families FIA_EBR (see 8.2), FIA_BVR (see 8.3), and FIA_BID (see 8.4) of Class FIA, specified in ISO/IEC 15408-2, which can be used in protection profiles and security targets in order to model the security mechanism of PAD for biometric enrolment, verification, and identification. The families are applied to the TOEs of either case in 6.3.1 of biometric recognition performance evaluation and to the TOEs of the third case in 6.3.2 for PAD evaluation.

Annex C provides explanatory information for the extended security functional components to Class FIA and shall be consulted when using the components identified in Clause 8.

NOTE 1 The Class FIA is a Class "Identification and authentication" specified in ISO/IEC 15408-2:2008 (see ISO/IEC 15408-2:2008, Clause 11, and also Annex A).

NOTE 2 From the viewpoint of PAD evaluation, the families provided in this clause are for a TOE of the third category classified in 6.3.2.

8.2 Enrolment of biometric reference (FIA_EBR)

8.2.1 Family behaviour

NOTE In ISO/IEC 15408-2, the title is "family behaviour".

This family defines enrolment mechanisms for biometric verification/identification supported by the TSF. This family also defines the required attributes on which the biometric enrolment mechanisms must be based.

8.2.2 Component levelling

Figure 7 shows the structure of this family.

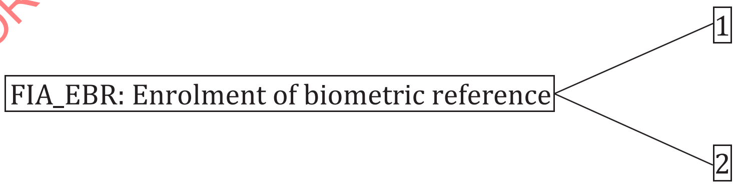

Figure 7 — FIA_EBR Enrolment of biometric reference family

FIA_EBR.1 check of biometric characteristics for enrolment, requires the TSF to prevent enrolment if presentation attack instruments are presented.

FIA_EBR.2 biometric enrolment with low failure to enrol rate, requires the TSF to prevent from enrolling only such biometric references of extremely good quality in order to achieve apparent good performance in biometric verification/identification afterwards.

8.2.3 Management of FIA_EBR.1

The following actions can be considered for the management functions in FMT:

a) the management of the TSF data, which include, for example, threshold values for quality scores to generate biometric reference by an administrator;

b) the management of the TSF data, which include, for example, values for detecting presentation attack instruments by an administrator.

8.2.4 Management of FIA_EBR.2

The following action can be considered for the management functions in FMT: the management of the TSF data, which include, for example, threshold values for quality scores to generate biometric reference by an administrator.

8.2.5 Audit of FIA_EBR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) minimal: rejection by the TSF of data that is checked as low quality or detected as presentation attack instrument;

b) basic: rejection or acceptance by the TSF of data that is quality checked or input to presentation attack detection subsystem;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for quality scores and detecting presentation attack instruments.

8.2.6 Audit of FIA_EBR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) minimal: rejection by the TSF of data that is checked as low quality;

b) basic: rejection or acceptance by the TSF of data that is quality checked;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for quality scores of biometric data for enrolment.

8.2.7 FIA_EBR.1 Check of biometric samples for enrolment

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_EBR.1.1

The TSF shall prevent use of non-artificial presentation attack instruments for enrolment of [assignment: *biometric characteristic*] that has been presented by any user of the TSF.

FIA_EBR.1.2

The TSF shall prevent use of artificial presentation attack instruments for enrolment of [assignment: *biometric characteristic*] that has been presented by any user of the TSF.

NOTE In ISO/IEC 15408-2, FIA_EBR.1.1 and FIA_EBR.1.2 would be numbered as 8.2.7.1 and 8.2.7.2 respectively.

8.2.8 FIA_EBR.2 Biometric enrolment with low failure to enrol rate

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_EBR.2.1

The TSF shall provide a mechanism to enrol biometric reference for [assignment: *biometric characteristic*] with the FTER not exceeding [assignment: *defined value*].

NOTE In ISO/IEC 15408-2, FIA_EBR.2.1 would be numbered as 8.2.8.1.

8.3 Biometric verification (FIA_BVR)

8.3.1 Family behaviour

This family defines biometric verification mechanisms supported by the TSF. This family also defines the required attributes on which the biometric verification mechanisms shall be based.

8.3.2 Component levelling

Figure 8 shows the structure of this family.

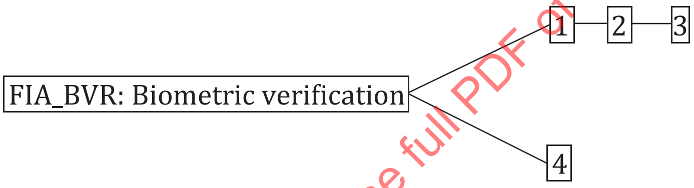

Figure 8 — FIA_BVR Biometric verification

FIA_BVR.1 biometric verification with high performance, requires the TSF to limit FMR and FNMR, or FAR and FRR respectively within a specified rate.

FIA_BVR.2 timing of the user authentication with biometric verification, allows a user to perform certain actions prior to the user authentication with biometric verification of the user's identity.

FIA_BVR.3 user authentication with biometric verification before any action, requires that users are authenticated with biometric verification before any other action is allowed by the TSF.

FIA_BVR.4 biometric verification not accepting presentation attack instruments, requires the biometric verification mechanism to be able to prevent the successful use of presentation attack instrument in a verification attempt.

8.3.3 Management of FIA_BVR.1

The following action can be considered for the management functions in FMT: the management of the TSF data (including the threshold values) by an administrator.

8.3.4 Management of FIA_BVR.2

The following actions can be considered for the management functions in FMT:

a) the management of the TSF data (including the threshold values) by an administrator;

b) managing of the list of the actions that can be taken before the user is authenticated.

8.3.5 Management of FIA_BVR.3

The following action can be considered for the management functions in FMT: the management of the TSF data (including the threshold values) by an administrator.

8.3.6 Management of FIA_BVR.4

The following action can be considered for the management functions in FMT: the management of the TSF data, which include, for example, values for detecting presentation attack instruments and for checking quality to generate biometric samples by an administrator.

NOTE The administrator is the administrator of the biometric system.

8.3.7 Audit of FIA_BVR.1

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: unsuccessful use of the biometric verification mechanism;

b) basic: all use of the biometric verification mechanism;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for biometric comparison scores used in biometric verification.

8.3.8 Audit of FIA_BVR.2

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: unsuccessful use of the user authentication mechanism with biometric verification;

b) basic: all use of the user authentication mechanism with biometric verification;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for biometric comparison scores used in biometric verification and all TSF mediated user actions performed before authentication with biometric verification of the user.

8.3.9 Audit of FIA_BVR.3

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: unsuccessful use of the user authentication mechanism with biometric verification;

b) basic: all use of the user authentication mechanism with biometric verification.

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for biometric comparison scores used in biometric verification.

8.3.10 Audit of FIA_BVR.4

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: rejection by the TSF of data that is checked as low quality or detected as presentation attack instrument;

b) basic: rejection or acceptance by the TSF of data that is quality checked or input to presentation attack detection subsystem;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for quality scores and detecting presentation attack instruments.

8.3.11 FIA_BVR.1 Biometric verification with high performance

Hierarchical to: No other components.

Dependencies: FIA_EBR.1 Check of biometric samples for enrolment

FIA_EBR.2 Biometric enrolment with low failure to enrol rate

FIA_BVR.1.1

The TSF shall provide a biometric verification mechanism for [assignment: *biometric characteristic*] to the user with the [selection: *FMR, FAR*] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*].

NOTE In ISO/IEC 15408-2, FIA_BVR.1.1 would be numbered as 8.3.11.1.

8.3.12 FIA_BVR.2 Timing of user authentication with biometric verification

Hierarchical to: FIA_BVR.1 biometric verification with high accuracy

Dependencies: FIA_UID.1 timing of identification

FIA_EBR.1 check of biometric samples for enrolment

FIA_EBR.2 biometric enrolment with low failure to enrol rate

FIA_BVR.2.1

The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated with biometric verification based on [assignment: *biometric characteristic*].

FIA_BVR.2.2

The TSF shall provide a user authentication mechanism with biometric verification based on [assignment: *biometric characteristic*] to the user with the [selection: *FMR, FAR*] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*] to require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

NOTE In ISO/IEC 15408-2, FIA_BVR.2.1 and FIA_BVR.2.2 would be numbered as 8.3.12.1 and 8.3.12.2 respectively.

8.3.13 FIA_BVR.3 User authentication with biometric verification before any action

Hierarchical to: FIA_BVR.2 timing of the user authentication with biometric verification

Dependencies: FIA_UID.1 timing of identification

FIA_EBR.1 check of biometric samples for enrolment

FIA_EBR.2 biometric enrolment with low failure to enrol rate

FIA_BVR.3.1

The TSF shall provide a user authentication mechanism with biometric verification based on [assignment: *biometric characteristic*] to the user with the [selection: FMR, FAR] not exceeding [assignment: defined value] and [selection: FNMR, FRR] not exceeding [assignment: defined value] to require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

NOTE In ISO/IEC 15408-2, FIA_BVR.3.1 would be numbered as 8.3.13.1.

8.3.14 FIA_BVR.4 Biometric verification not accepting presentation attack instruments

Hierarchical to: No other components.

Dependencies: FIA_EBR.1 check of biometric samples for enrolment

FIA_BVR.4.1

The TSF shall prevent use of non-artificial presentation attack instruments for [assignment: *biometric characteristic*] from being successfully verified.

FIA_BVR.4.2

The TSF shall prevent use of artificial presentation attack instruments for [assignment: *biometric characteristic*] from being successfully verified.

NOTE In ISO/IEC 15408-2, FIA_BVR.4.1 and FIA_BVR.4.2 would be numbered as 8.3.14.1 and 8.3.14.2 respectively.

8.4 Biometric identification (FIA_BID)

8.4.1 Family behaviour

This family defines biometric identification mechanisms supported by the TSF. This family also defines the required attributes on which the biometric identification mechanisms shall be based.

8.4.2 Component levelling

Figure 9 shows the structure of this family.

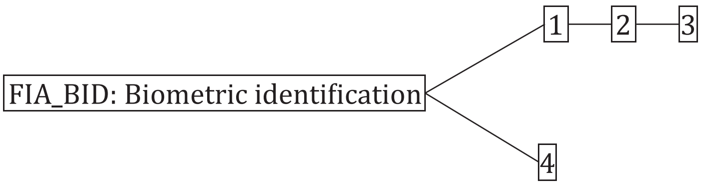

Figure 9 — FIA_BID Biometric identification

FIA_BID.1 biometric identification with high performance, requires the TSF to limit FPIR and FNIR respectively within a specified rate.

FIA_BID.2 timing of the biometric identification, allows a user to perform certain actions prior to the biometric identification.

FIA_BID.3 biometric identification before any action, requires that users are biometriccally identified before any other action is allowed by the TSF.

FIA_BID.4 biometric identification not accepting presentation attack instruments, requires the biometric identification mechanism to be able to prevent the successful use of presentation attack instrument in a biometric identification attempt.

8.4.3 Management of FIA_BID.1

The following action can be considered for the management functions in FMT: the management of the TSF data (including the threshold values) by an administrator.

8.4.4 Management of FIA_BID.2

The following actions can be considered for the management functions in FMT:

a) the management of the TSF data (including the threshold values) by an administrator;

b) managing of the list of the actions that can be taken before the user is biometrically identified.

8.4.5 Management of FIA_BID.3

The following action can be considered for the management functions in FMT: the management of the TSF data (including the threshold values) by an administrator.

8.4.6 Management of FIA_BID.4

The following action can be considered for the management functions in FMT: the management of the TSF data, which include, for example, values for detecting presentation attack instruments and for checking quality to generate biometric samples by an administrator.

NOTE The administrator is the administrator of the biometric system.

8.4.7 Audit of FIA_BID.1

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: unsuccessful use of the biometric identification mechanism;

b) basic: all use of the biometric identification mechanism;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for biometric comparison scores used in biometric identification.

8.4.8 Audit of FIA_BID.2

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: unsuccessful use of the biometric identification mechanism;

b) basic: all use of the biometric identification mechanism;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for biometric comparison scores used in biometric identification and all TSF mediated user actions performed before biometric identification of the user.

8.4.9 Audit of FIA_BID.3

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: unsuccessful use of the biometric identification mechanism;

b) basic: all use of the biometric identification mechanism.

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for biometric comparison scores used in biometric identification.

8.4.10 Audit of FIA_BID.4

The following actions should be auditable if FAU_GEN security audit data generation is included in the PP/ST:

a) minimal: rejection by the TSF of data that is checked as low quality or detected as presentation attack instrument;

b) basic: rejection or acceptance by the TSF of data that is quality checked or input to presentation attack detection subsystem;

c) detailed: identification of the changes to the TSF data, which include, for example, threshold values for quality scores and detecting presentation attack instruments.

8.4.11 FIA_BID.1 Biometric identification with high performance

Hierarchical to:	No other components.
Dependencies:	FIA_EBR.1 check of biometric samples for enrolment
	FIA_EBR.2 biometric enrolment with low failure to enrol rate

FIA_BID.1.1

The TSF shall provide a biometric identification mechanism based on [assignment: *biometric characteristics*] to the user with the FPIR not exceeding [assignment: *defined value*] and FNIR not exceeding [assignment: *defined value*].

NOTE In ISO/IEC 15408-2, FIA_BID.1.1 would be numbered as 8.4.11.1.

8.4.12 FIA_BID.2 Timing of biometric identification

Hierarchical to:	FIA_BID.1 high accuracy biometric identification
Dependencies:	FIA_EBR.1 check of biometric samples for enrolment
	FIA_EBR.2 biometric enrolment with low failure to enrol rate

FIA_BID.2.1

The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is biometrically identified based on [assignment: *biometric characteristics*].

FIA_BID.2.2

The TSF shall provide a biometric identification mechanism based on [assignment: *biometric characteristics*] to the user with the FPIR not exceeding [assignment: *defined value*] and FNIR not exceeding [assignment: *defined value*] to require each user to be biometrically identified before allowing any other TSF-mediated actions on behalf of that user.

NOTE In ISO/IEC 15408-2, FIA_BID.2.1 and FIA_BID.2.2 would be numbered as 8.4.12.1 and 8.4.12.2 respectively.

8.4.13 FIA_BID.3 Biometric identification before any action

Hierarchical to: FIA_BID.2 timing of the user authentication with biometric identification

Dependencies: FIA_EBR.1 check of biometric samples for enrolment

FIA_EBR.2 biometric enrolment with low failure to enrol rate

FIA_BID.3.1

The TSF shall provide a biometric identification mechanism based on [assignment: *biometric characteristic*] to the user with the FPIR not exceeding [assignment: *defined value*] and FNIR not exceeding [assignment: *defined value*] to require each user to be biometrically identified before allowing any other TSF-mediated actions on behalf of that user.

NOTE In ISO/IEC 15408-2, FIA_BID.3.1 would be numbered as 8.4.13.1.

8.4.14 FIA_BID.4 Biometric identification not accepting presentation attack instruments

Hierarchical to: No other components.

Dependencies: FIA_EBR.1 check of biometric samples for enrolment

FIA_BID.4.1

The TSF shall prevent use of non-artificial presentation attack instruments for [assignment: *biometric characteristic*] from being successfully identified.

FIA_BID.4.2

The TSF shall prevent use of artificial presentation attack instruments for [assignment: *biometric characteristic*] from being successfully identified.

NOTE In ISO/IEC 15408-2, FIA_BID.4.1 and FIA_BID.4.2 would be numbered as 8.4.14.1 and 8.4.14.2 respectively.

9 Supplementary activities to ISO/IEC 18045 on Class APE: Protection Profile evaluation

Table 1 lists the supplementary activities to the work units in APE_INT which shall be applied only to the security evaluation of PAD (see also D.1.1). There are no other supplementary activities in Class APE.

Table 1 — Supplement to APE_INT (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
APE_INT.1.1E	APE_INT.1-1	None
	APE_INT.1-2	None
	APE_INT.1-3	The evaluator ***shall examine*** the TOE overview to determine that the TOE provides presentation attack detection mechanism.
	APE_INT.1-4	The evaluator ***shall examine*** the TOE overview to determine that it does not claim error rates for presentation attack detection mechanism.
	APE_INT.1-5	None

NOTE It applies also to TOEs which do not claim PAD resistance, in order to check if the evaluator needs to take this feature in account during AVA for biometric recognition performance.

10 Supplementary activities to ISO/IEC 18045 on Class ASE: Security Target evaluation

Table 2 and Table 3 list the supplementary activities to the work units in ASE_INT (see also D.1.1). There are no other supplementary activities in Class ASE.

Table 2 — Supplement to ASE_INT (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ASE_INT.1.1E	ASE_INT.1-1	None
	ASE_INT.1-2	None
	ASE_INT.1-3	None
	ASE_INT.1-4	The evaluator ***shall examine*** the TOE reference to determine that clearly identifies the modality that the TOE can be used for.
	ASE_INT.1-5	None
	ASE_INT.1-6	None
	ASE_INT.1-7	None
	ASE_INT.1-8	None
	ASE_INT.1-9	None
	ASE_INT.1-10	None

Table 3 — Supplement to ASE_INT (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ASE_INT.1.1E	ASE_INT.1-1	None
	ASE_INT.1-2	None
	ASE_INT.1-3	None
	ASE_INT.1-4	The evaluator ***shall examine*** the TOE reference to determine that clearly identifies the modality that the TOE can be used for.
	ASE_INT.1-5	The evaluator ***shall examine*** the TOE overview to determine that the TOE provides presentation attack detection mechanism.
	ASE_INT.1-6	None
	ASE_INT.1-7	The evaluator ***shall examine*** the TOE overview to determine that it doesn't claim error rates for presentation attack detection mechanism.
	ASE_INT.1-8	None
	ASE_INT.1-9	None
	ASE_INT.1-10	None

11 Supplementary activities to ISO/IEC 18045 on Class ADV: Development

11.1 Supplementary activities to security architecture ADV_ARC

Table 4 lists the supplementary activities supplemented to the work units in the sub-activity action ADV_ARC1.1E which shall be applied only to the security evaluation of PAD. ADV_ARC.1-5 is applied to the TOE which provides biometric recognition as well as PAD (see also D.2.1).

Table 4 — Supplement to ADV_ARC (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_ARC.1.1E	ADV_ARC.1-1	None
	ADV_ARC.1-2	None
	ADV_ARC.1-3	None
	ADV_ARC.1-4	None
	ADV_ARC.1-5	The evaluator ***shall examine*** the security architecture documentation with regard to the mechanisms that ensure that the capture device and the PAD are being presented the same biometric characteristic(s)

11.2 Supplementary activities to functional specification ADV_FSP

11.2.1 Supplementary activities to evaluation of sub-activity ADV_FSP.1

There are no supplementary activities to evaluation of sub-activity ADV_FSP.1.

11.2.2 Supplementary activities to evaluation of sub-activity ADV_FSP.2

Table 5 and Table 6 list the supplementary activities supplemented to the work units in the sub-activity action ADV_FSP.2.1E (See also D.2.2). There are no other supplementary activities supplemented to the evaluation of sub-activity action ADV_FSP.2.2E.

Table 5 — Supplement to ADV_FSP.2.1E (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.2.1E	ADV_FSP.2-1	None
	ADV_FSP.2-2	None
	ADV_FSP.2-3	The evaluator ***shall examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.2-4	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely identifies security relevant parameters for capture devices.
	ADV_FSP.2-5	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters associated with the TSFI for capture devices.
	ADV_FSP.2-6	None
	ADV_FSP.2-7	None
	ADV_FSP.2-8	None

Table 6 — Supplement to ADV_FSP.2.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.2.1E	ADV_FSP.2-1	The evaluator ***shall examine*** the functional specification to determine that the various mechanisms used for presentation attack detection are described in terms of TSFIs.
	ADV_FSP.2-2	None
	ADV_FSP.2-3	The evaluator ***shall examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.2-4	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely identifies security relevant parameters for capture devices.
	ADV_FSP.2-5	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters associated with the TSFI for capture devices.
	ADV_FSP.2-6	None
	ADV_FSP.2-7	The evaluator ***shall examine*** the presentation of the TSFI to determine that it doesn't provide feedback on the decision of the presentation attack detection to the user if the TOE contains more than PAD subsystem.
	ADV_FSP.2-8	None

11.2.3 Supplementary activities to Evaluation of sub-activity ADV_FSP.3

Table 7 and Table 8 list the supplementary activities supplemented to the work units in the sub-activity action ADV_FSP.3.1E (see also D.2.2). There are no other supplementary activities supplemented to the evaluation of sub-activity action ADV_FSP.3.2E.

Table 7 — Supplement to ADV_FSP.3.1E (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.3.1E	ADV_FSP.3-1	None
	ADV_FSP.3-2	None
	ADV_FSP.3-3	The evaluator ***shall examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.3-4	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely identifies security relevant parameters for capture devices.
	ADV_FSP.3-5	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters associated with the TSFI for capture devices.
	ADV_FSP.3-6	None
	ADV_FSP.3-7	None
	ADV_FSP.3-8	None
	ADV_FSP.3-9	None

Table 8 — Supplement to ADV_FSP.3.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.3.1E	ADV_FSP.3-1	The evaluator ***shall examine*** the functional specification to determine that the various mechanisms used for presentation attack detection are described in terms of TSFIs.
	ADV_FSP.3-2	None
	ADV_FSP.3-3	The evaluator ***shall examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.3-4	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely identifies security relevant parameters for capture devices.
	ADV_FSP.3-5	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters associated with the TSFI for capture devices.
	ADV_FSP.3-6	None
	ADV_FSP.3-7	The evaluator ***shall examine*** the presentation of the TSFI to determine that it doesn’t provide feedback on the decision of the presentation attack detection to the user if the TOE contains more than PAD subsystem.
	ADV_FSP.3-8	None
	ADV_FSP.3-9	None

11.2.4 Supplementary activities to Evaluation of sub-activity ADV_FSP.4

Table 9 and Table 10 list the supplementary activities supplemented to the work units in the sub-activity action ADV_FSP.4.1E (see also D.2.2). There are no other supplementary activities supplemented to the evaluation of sub-activity action ADV_FSP.4.2E.

Table 9 — Supplement to ADV_FSP.4.1E (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.4.1E	ADV_FSP.4-1	None
	ADV_FSP.4-2	None
	ADV_FSP.4-3	The evaluator ***shall examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.4-4	None
	ADV_FSP.4-5	None
	ADV_FSP.4-6	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters associated with the TSFI for capture devices.
	ADV_FSP.4-7	None
	ADV_FSP.4-8	None
	ADV_FSP.4-9	None
	ADV_FSP.4-10	None

Table 10 — Supplement to ADV_FSP.4.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.4.1E	ADV_FSP.4-1	The evaluator ***shall examine*** the functional specification to determine that the various mechanisms used for presentation attack detection are described in terms of TSFIs.
	ADV_FSP.4-2	None
	ADV_FSP.4-3	The evaluator ***shall examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.4-4	None
	ADV_FSP.4-5	None
	ADV_FSP.4-6	The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters associated with the TSFI for capture devices.
	ADV_FSP.4-7	None
	ADV_FSP.4-8	The evaluator ***shall examine*** the presentation of the TSFI to determine that it doesn't provide feedback on the decision of the presentation attack detection to the user if the TOE contains more than PAD subsystem.
	ADV_FSP.4-9	None
	ADV_FSP.4-10	None

11.3 Supplementary activities to TOE design ADV_TDS

11.3.1 Supplementary activities to evaluation of sub-activity ADV_TDS.1

Table 11 lists the supplementary activities supplemented to the work units in the sub-activity action ADV_TDS.1.1E which shall be applied only to the security evaluation of PAD (see also D.2.4). There are no other supplementary activities supplemented to the evaluation of sub-activity action ADV_TDS.1.2E.

Table 11 — Supplement to ADV_TDS.1.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_TDS.1.1E	ADV_TDS.1-1	None
	ADV_TDS.1-2	None
	ADV_TDS.1-3	None
	ADV_TDS.1-4	The evaluator ***shall examine*** the TOE design to determine that it describes biometric properties and mechanisms which are used to detect presentation attacks are described on the subsystem level, that is, the processing of signals acquired by the capture devices used for presentation attack detection and the transformation of these signals into classification of presentation attack.
	ADV_TDS.1-5	The evaluator ***shall examine*** the TOE design to determine that the interactions between the presentation attack detection mechanism and the capturing functionality are described at the subsystem level.
	ADV_TDS.1-6	None

11.3.2 Supplementary activities to evaluation of sub-activity ADV_TDS.2

Table 12 lists the supplementary activities supplemented to the work units in the sub-activity action ADV_TDS.2.1E which shall be applied only to the security evaluation of PAD (see also D.2.4). There are no other supplementary activities supplemented to the evaluation of sub-activity action ADV_TDS.2.2E.

Table 12 — Supplement to ADV_TDS.2.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_TDS.2.1E	ADV_TDS.2-1	None
	ADV_TDS.2-2	None
	ADV_TDS.2-3	None
	ADV_TDS.2-4	The evaluator ***shall examine*** the TOE design to determine that it describes biometric properties and mechanisms which are used to detect presentation attacks are described on the subsystem level, that is, the processing of signals acquired by the capture devices used for presentation attack detection and the transformation of these signals into classification of presentation attack.
	ADV_TDS.2-5	None
	ADV_TDS.2-6	None
	ADV_TDS.2-7	The evaluator ***shall examine*** the TOE design to determine that the interactions between the presentation attack detection mechanism and the capturing functionality are described on the subsystem level.
	ADV_TDS.2-8	None

11.3.3 Supplementary activities to evaluation of sub-activity ADV_TDS.3

Table 13 lists the supplementary activities supplemented to the work units in the sub-activity action ADV_TDS.3.1E which shall be applied only to the security evaluation of PAD (see also D.2.4). There are no other supplementary activities supplemented to the evaluation of sub-activity action ADV_TDS.3.2E.

Table 13 — Supplement to ADV_TDS.3.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ADV_TDS.3.1E	ADV_TDS.3-1	None
	ADV_TDS.3-2	None
	ADV_TDS.3-3	None
	ADV_TDS.3-4	The evaluator ***shall examine*** the TOE design to determine that it describes biometric properties and mechanisms which are used to detect presentation attacks at the module level, that is, the processing of signals acquired by the capture devices used for presentation attack detection and the transformation of these signals into classification of presentation attack.
	ADV_TDS.3-5	None
	ADV_TDS.3-6	The evaluator ***shall examine*** the TOE design to determine that the interactions between the presentation attack detection mechanism and the capturing functionality are described at the module level.
	ADV_TDS.3-7	None
	ADV_TDS.3-8	None
	ADV_TDS.3-9	None
	ADV_TDS.3-10	None
	ADV_TDS.3-11	None
	ADV_TDS.3-12	None
	ADV_TDS.3-13	None
	ADV_TDS.3-14	None

12 Supplementary activities to ISO/IEC 18045 on Class AGD: Guidance documents

12.1 Supplementary activities to operational user guidance AGD_OPE

Table 14 and Table 15 list the supplementary activities supplemented to the work units in the sub-activity action AGD_OPE.1.1E (see also D.3.1). There are no other supplementary activities supplemented to the evaluation of sub-activity action AGD_OPE.1.2E.

Table 14 — Supplement to AGD_OPE.1.1E (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
AGD_OPE.1.1E	AGD_OPE.1-1	None
	AGD_OPE.1-2	The evaluator ***shall examine*** the operational user guidance to determine that it describes the process of presenting biometric characteristics to the TOE if the capture devices are part of the TOE.
	AGD_OPE.1-3	The evaluator ***shall examine*** the operational user guidance to determine that it describes the secure configuration of parameters for biometric recognition.
	AGD_OPE.1-4	None
	AGD_OPE.1-5	None
	AGD_OPE.1-6	None
	AGD_OPE.1-7	None
	AGD_OPE.1-8	None

Table 15 — Supplement to AGD_OPE.1.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
AGD_OPE.1.1E	AGD_OPE.1-1	None
	AGD_OPE.1-2	The evaluator ***shall examine*** the operational user guidance to determine that it describes the process of presenting biometric characteristics to the TOE if the capture devices are part of the TOE.
	AGD_OPE.1-3	The evaluator ***shall examine*** the operational user guidance to determine that it describes the secure configuration of presentation attack detection parameters.
	AGD_OPE.1-4	The evaluator ***shall examine*** the operational user guidance to determine that it describes alternative procedures that allow an operator to manually override the decision of the presentation attack detection or of the biometric recognition subsystem.
	AGD_OPE.1-5	The evaluator ***shall examine*** the operational user guidance to determine that it describes mode of operation of the TOE that an operator can manually override the decision of the presentation attack detection.
	AGD_OPE.1-6	None
	AGD_OPE.1-7	None
	AGD_OPE.1-8	None

12.2 Supplementary activities to preparative procedures AGD_PRE

Table 16 and Table 17 list the supplementary activities supplemented to the work units in the sub-activity action AGD_PRE.1.1E which shall be applied only to the security evaluation of PAD (see also D.3.2). There are no other supplementary activities supplemented to the evaluation of sub-activity action AGD_PRE.1.2E.

Table 16 — Supplement to AGD_PRE.1.1E (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
AGD_PRE.1.1E	AGD_PRE.1-1	None
	AGD_PRE.1-2	The evaluator ***shall examine*** the provided installation procedures to determine that they describe, in particular, parameters that modify the security mechanism of biometric recognition (e.g. a threshold) and that shall be configured before the initial usage of the TOE.

Table 17 — Supplement to AGD_PRE.1.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
AGD_PRE.1.1E	AGD_PRE.1-1	None
	AGD_PRE.1-2	The evaluator ***shall examine*** the provided installation procedures to determine that they describe, in particular, parameters that modify the security mechanism of presentation attack detection (e.g. a threshold) and that shall be configured before the initial usage of the TOE.

13 Supplementary activities to ISO/IEC 18045 on Class ALC: Life-cycle support

13.1 Supplementary activities to CM support ALC_CMS

There are no supplementary activities supplemented to evaluation of sub-activity ALC_CMS.1, evaluation of sub-activity ALC_CMS.2, evaluation of sub-activity ALC_CMS.3, and evaluation of sub-activity ALC_CMS.5.

Table 18 lists the supplementary activities supplemented to the work units in the sub-activity action ALC_CMS.4.1E which shall be applied only to the security evaluation of PAD (see also D.4.1).

Table 18 — Supplement to ALC_CMS.4.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ALC_CMS.4.1E	ALC_CMS.4-1	The evaluator ***shall check*** that the documentation used to record details of reported security flaws associated with the implementation includes those that the presentation attack detection system did not detect PAIs.
	ALC_CMS.4-2	None
	ALC_CMS.4-3	None

13.2 Supplementary activities to Delivery ALC_DEL

Table 19 lists the supplementary activities supplemented to the work units in the sub-activity action ALC_DEL.1.1E which shall be applied only to the security evaluation of PAD (see also D.4.2).

Table 19 — Supplement to ALC_DEL.1.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ALC_DEL.1.1E	ALC_DEL.1-1	The evaluator ***shall examine*** the delivery documentation to determine that it describes whether the TOE is readily available for all kind of customers or only purchased by restricted customers.
	ALC_DEL.1-2	None

13.3 Supplementary activities to flaw remediation ALC_FLR

The following shall be applied to all the work units in ALC_FLR.

The evaluator shall determine that PAIs which are falsely accepted by the presentation attack detection system are considered being security flaws in the developers' processes (see also D.4.3).

14 Supplementary activities to ISO/IEC 18045 on Class ATE: Tests

14.1 Supplementary activities to functional tests ATE_FUN

Table 20 and Table 21 list the supplementary activities supplemented to the work units in the sub-activity action ATE_FUN.1.1E (see also D.5.1).

Table 20 — Supplement to ATE_FUN.1.1E (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ATE_FUN.1.1E	ATE_FUN.1-1	The evaluator shall ***check*** that the test documentation satisfies the relevant requirements from ISO/IEC 19795. The evaluator ***shall explain*** any deviation from the test procedures specified in ISO/IEC 19795 and ***shall describe*** any potential effects and implications for the test results in the test documentation.
	ATE_FUN.1-2	The evaluator ***shall check*** that the test plan provides information on dataset or test crew used for the developer tests on biometric recognition performances.
	ATE_FUN.1-3	None
	ATE_FUN.1-4	None
	ATE_FUN.1-5	None
	ATE_FUN.1-6	None
	ATE_FUN.1-7	None

Table 21 — Supplement to ATE_FUN.1.1E (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ATE_FUN.1.1E	ATE_FUN.1-1	None
	ATE_FUN.1-2	The evaluator ***shall examine*** that the test plan to determine that it describes information on the attack type that were created by the developer for the tests including detailed information on the PAI species such as material information and construction manuals, method of interaction with the capture device, and whether it is targeted against concealer or impostor attack.
	ATE_FUN.1-3	The evaluator ***shall examine*** the test plan to determine that potential presentation attack detection parameters are correctly configured according to the TOE configuration described in the ST.
	ATE_FUN.1-4	None
	ATE_FUN.1-5	The evaluator ***shall examine*** the test documentation to determine that all expected error rates on presentation attack detection results are included.
	ATE_FUN.1-6	The evaluator ***shall check*** that the actual test results of error rates on presentation attack detection in the test documentation are consistent with those expected in the test documentation.
	ATE_FUN.1-7	The evaluator ***shall report*** the efforts of the developer for presentation attack detection mechanism tests in terms of number and description of the attack types, PAI species, and test size.

See also ISO/IEC 19989-3.

14.2 Supplementary activities to independent testing ATE_IND

14.2.1 General

There are no supplementary activities supplemented to evaluation of sub-activity ATE_IND.3.

14.2.2 Supplementary activities to evaluation of sub-activity ATE_IND.1

Table 22 and Table 23 list the supplementary activities supplemented to the work units in ATE_IND.1 (see also D.5.2).

Table 22 — Supplement to ATE_IND.1 (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ATE_IND.1.1E	ATE_IND.1-1	None
	ATE_IND.1-2	None
ATE_IND.1.2E	ATE_IND.1-3	The evaluator ***shall devise*** independent testing for performance evaluation setting up a test crew or a test dataset.
	ATE_IND.1-4	The evaluator ***shall produce*** test documentation for performance evaluation which satisfies the relevant requirements from ISO/IEC 19795. The evaluator ***shall explain*** any deviation from the test procedures specified in ISO/IEC 19795 and ***shall describe*** any potential effects and implications for the test results in the test documentation.
	ATE_IND.1-5	The evaluator ***shall conduct*** testing using test crew which the evaluator arranged or test data which the evaluator possesses.
	ATE_IND.1-6	The evaluator ***shall record*** information of test crew or test data as specified in ISO/IEC 19795.
	ATE_IND.1-7	None
	ATE_IND.1-8	The evaluator ***shall report*** in the ETR the evaluator testing effort on biometric recognition performance in terms of test size, time spent, and also dataset characteristics.

Table 23 — Supplement to ATE_IND.1 (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ATE_IND.1.1E	ATE_IND.1-1	The evaluator ***shall examine*** the TOE to determine that the potential presentation attack detection parameters are correctly configured according to the TOE configuration described in the ST.
	ATE_IND.1-2	None
ATE_IND.1.2E	ATE_IND.1-3	The evaluator ***shall devise*** a test subset in which the evaluator uses or rebuilds PAIs created by the developer in a different manner from that done by the developer, such as presenting PAIs in a different manner. In addition, the evaluator ***should devise*** their own test subset. The evaluator ***should consider*** modifying PAIs created by the developer for testing. The evaluator ***should consider*** disabling the PAD mechanism in the TOE to refine PAIs so that they can falsely accepted by the biometric verification mechanism of the TOE, if a TOE whose PAD mechanism can be disabled is available for testing.
	ATE_IND.1-4	None
	ATE_IND.1-5	None
	ATE_IND.1-6	The evaluator ***shall record*** PAI modification and its usage.
	ATE_IND.1-7	None
	ATE_IND.1-8	The evaluator ***shall report*** in the ETR the evaluator testing effort on presentation attack detection mechanism in terms of number and description of attack types, PAI species, and test size.

14.2.3 Supplementary activities to Evaluation of sub-activity ATE_IND.2

Table 24 and Table 25 list the supplementary activities supplemented to the work units in ATE_IND.2 (see also D.5.2).

Table 24 — Supplement to ATE_IND.2 (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
ATE_IND.2.1E	ATE_IND.2-1	None
	ATE_IND.2-2	None
	ATE_IND.2-3	None
ATE_IND.2.2E	ATE_IND.2-4	None
	ATE_IND.2-5	None
ATE_IND.2.3E	ATE_IND.2-6	The evaluator ***shall devise*** independent testing for performance evaluation setting up a test crew or a test dataset.
	ATE_IND.2-7	The evaluator ***shall produce*** test documentation for performance evaluation which satisfies the relevant requirements from ISO/IEC 19795. The evaluator ***shall explain*** any deviation from the test procedures specified in ISO/IEC 19795 and ***shall describe*** any potential effects and implications for the test results in the test documentation.
	ATE_IND.2-8	The evaluator ***shall conduct*** testing using test crew which the evaluator arranged or test data which the evaluator possesses.
	ATE_IND.2-9	The evaluator ***shall record*** information of test crew or test data as specified in ISO/IEC 19795.
	ATE_IND.2-10	None
	ATE_IND.2-11	The evaluator ***shall report*** in the ETR the evaluator testing effort on biometric recognition performance in terms of test size, time spent, and also dataset characteristics.

Table 25 — Supplement to ATE_IND.2 (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
ATE_IND.2.1E	ATE_IND.2-1	The evaluator ***shall examine*** the TOE to determine that the potential presentation attack detection parameters are correctly configured according to the TOE configuration described in the ST.
	ATE_IND.2-2	None
	ATE_IND.2-3	None
ATE_IND.2.2E	ATE_IND.2-4	The evaluator ***shall conduct*** testing using or rebuilding the PAIs created by the developer.
	ATE_IND.2-5	None

Table 25 *(continued)*

Evaluator action element	Work unit	Supplementary activities
ATE_IND.2.3E	ATE_IND.2-6	The evaluator ***shall devise*** a test subset in which the evaluator uses or rebuilds PAIs created by the developer in a different manner from that done by the developer, such as presenting PAIs in a different manner. In addition, the evaluator ***shall devise*** their own test subset. The evaluator ***should consider*** modifying PAIs created by the developer for testing. The evaluator ***should consider*** disabling the PAD mechanism in the TOE to refine PAIs so that they can falsely accepted by the biometric verification mechanism of the TOE, if a TOE whose PAD mechanism can be disabled is available for testing.
	ATE_IND.2-7	None
	ATE_IND.2-8	None
	ATE_IND.2-9	The evaluator ***shall record*** PAI modification and its usage.
	ATE_IND.2-10	None
	ATE_IND.2-11	The evaluator ***shall report*** in the ETR the evaluator testing effort on presentation attack detection mechanism in terms of number and description of attack types, PAI species, and test size.

See also ISO/IEC 19989-3.

15 Supplementary activities to ISO/IEC 18045 on Class AVA: Vulnerability assessment

15.1 General

There are no supplementary activities supplemented to evaluation of sub-activity AVA_VAN.1 and evaluation of sub-activity AVA_VAN.5.

15.2 Supplementary activities to vulnerability analysis AVA_VAN

15.2.1 Supplementary activities to evaluation of sub-activity AVA_VAN.2

Table 26 and Table 27 list the supplementary activities supplemented to the work units in AVA_VAN.2 (see also D.6.1).

Table 26 — Supplement to AVA_VAN.2 (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.2.1E	AVA_VAN.2-1	None
	AVA_VAN.2-2	None
AVA_VAN.2.2E	AVA_VAN.2-3	None
AVA_VAN.2.3E	AVA_VAN.2-4	None
	AVA_VAN.2-5	None

Table 26 *(continued)*

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.2.4E	AVA_VAN.2-6	The evaluator ***shall devise*** penetration testing, also referencing ISO/IEC 19989-2 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.2-7	None
	AVA_VAN.2-8	None
	AVA_VAN.2-9	None
	AVA_VAN.2-10	None
	AVA_VAN.2-11	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-2 to determine attack potentials of attacks against biometric recognition performance.
	AVA_VAN.2-12	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-2 to determine attack potentials of attacks against biometric recognition performance.

NOTE Penetration testing is a term used in ISO/IEC 15408-3.

Table 27 — Supplement to AVA_VAN.2 (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.2.1E	AVA_VAN.2-1	The evaluator ***shall examine*** the TOE to determine that the test configuration of potential presentation attack detection parameters is consistent with the configuration under evaluation as described in the ST.
	AVA_VAN.2-2	None
AVA_VAN.2.2E	AVA_VAN.2-3	None
AVA_VAN.2.3E	AVA_VAN.2-4	The evaluator ***shall conduct*** a reference to ISO/IEC 19989-3 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.2-5	None
AVA_VAN.2.4E	AVA_VAN.2-6	The evaluator ***shall devise*** penetration testing, also referencing ISO/IEC 19989-3 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.2-7	The evaluator ***shall include*** construction manuals into the penetration test documentation for the PAIs that were built for penetration testing.
	AVA_VAN.2-8	None
	AVA_VAN.2-9	The evaluator ***shall record*** the PAI construction and usage.
	AVA_VAN.2-10	None
	AVA_VAN.2-11	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-3 to determine attack potentials of presentation attacks.
	AVA_VAN.2-12	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-3 to determine attack potentials of presentation attacks.

15.2.2 Supplementary activities to evaluation of sub-activity AVA_VAN.3

Table 28 and Table 29 list the supplementary activities supplemented to the work units in AVA_VAN.3 (see also D.6.1).

Table 28 — Supplement to AVA_VAN.3 (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.3.1E	AVA_VAN.3-1	None
	AVA_VAN.3-2	None

Table 28 *(continued)*

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.3.2E	AVA_VAN.3-3	None
AVA_VAN.3.3E	AVA_VAN.3-4	None
	AVA_VAN.3-5	None
AVA_VAN.3.4E	AVA_VAN.3-6	The evaluator ***shall devise*** penetration testing, also referencing ISO/IEC 19989-2 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.3-7	None
	AVA_VAN.3-8	None
	AVA_VAN.3-9	None
	AVA_VAN.3-10	None
	AVA_VAN.3-11	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-2 to determine attack potentials of attacks against biometric recognition performance.
	AVA_VAN.3-12	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-2 to determine attack potentials of attacks against biometric recognition performance.

Table 29 — Supplement to AVA_VAN.3 (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.3.1E	AVA_VAN.3-1	The evaluator ***shall examine*** the TOE to determine that the test configuration of potential presentation attack detection parameters is consistent with the configuration under evaluation as described in the ST.
	AVA_VAN.3-2	None
AVA_VAN.3.2E	AVA_VAN.3-3	None
AVA_VAN.3.3E	AVA_VAN.3-4	The evaluator ***shall conduct*** a reference to ISO/IEC 19989-3 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.3-5	None
AVA_VAN.3.4E	AVA_VAN.3-6	The evaluator ***shall devise*** penetration testing, also referencing ISO/IEC 19989-3 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.3-7	The evaluator ***shall include*** construction manuals into the penetration test documentation for the PAIs that were built for penetration testing.
	AVA_VAN.3-8	None
	AVA_VAN.3-9	The evaluator ***shall record*** the PAI construction and usage.
	AVA_VAN.3-10	None
	AVA_VAN.3-11	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-3 to determine attack potentials of presentation attacks.
	AVA_VAN.3-12	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-3 to determine attack potentials of presentation attacks.

15.2.3 Supplementary activities to evaluation of sub-activity AVA_VAN.4

Table 30 and Table 31 list the supplementary activities supplemented to the work units in AVA_VAN.4 (see also D.6.1).

Table 30 — Supplement to AVA_VAN.3 (applied to biometric recognition performance)

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.4.1E	AVA_VAN.4-1	None
	AVA_VAN.4-2	None
AVA_VAN.4.2E	AVA_VAN.4-3	None
AVA_VAN.4.3E	AVA_VAN.4-4	None
	AVA_VAN.4-5	None
AVA_VAN.4.4E	AVA_VAN.4-6	The evaluator ***shall devise*** penetration testing, also referencing ISO/IEC 19989-2 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.4-7	None
	AVA_VAN.4-8	None
	AVA_VAN.4-9	None
	AVA_VAN.4-10	None
	AVA_VAN.4-11	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-2 to determine attack potentials of attacks against biometric recognition performance.
	AVA_VAN.4-12	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-2 to determine attack potentials of attacks against biometric recognition performance.

Table 31 — Supplement to AVA_VAN.3 (applied to PAD)

Evaluator action element	Work unit	Supplementary activities
AVA_VAN.4.1E	AVA_VAN.4-1	The evaluator ***shall examine*** the TOE to determine that the test configuration of potential presentation attack detection parameters is consistent with the configuration under evaluation as described in the ST.
	AVA_VAN.4-2	None
AVA_VAN.4.2E	AVA_VAN.4-3	None
AVA_VAN.4.3E	AVA_VAN.4-4	The evaluator ***shall conduct*** a reference to ISO/IEC 19989-3 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.4-5	None
AVA_VAN.4.4E	AVA_VAN.4-6	The evaluator ***shall devise*** penetration testing, also referencing ISO/IEC 19989-3 to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.4-7	The evaluator ***shall include*** construction manuals into the penetration test documentation for the PAIs that were built for penetration testing.
	AVA_VAN.4-8	None
	AVA_VAN.4-9	The evaluator ***shall record*** the PAI construction and usage.
	AVA_VAN.4-10	None
	AVA_VAN.4-11	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-3 to determine attack potentials of presentation attacks.
	AVA_VAN.4-12	The evaluator ***shall refer*** to Annex F and the examples in ISO/IEC 19989-3 to determine attack potentials of presentation attacks.

Annex A
(informative)

Introduction to the basic concepts of ISO/IEC 15408

A.1 General

This annex aims to provide a short introduction to the formal language that is used in the ISO/IEC 15408 series to enable the readers who are not familiar with ISO/IEC 15408 series to understand this document. It does not intend to provide the readers with guidance for the principal use of the ISO/IEC 15408 series.

Within the ISO/IEC 15408 series, the target of evaluation (TOE) is the product or system that is the subject of the evaluation. The TOE is characterized through the security target (ST), i.e. a document that identifies the security functional requirements (SFR) and security assurance requirements (SAR) and may refer to one or more protection profiles (PP), i.e. documents that identify the SFR and SAR for a class of security products. In the ISO/IEC 15408 series, a protection profile behaves to a security target for a concrete product as a class does to an object in object-oriented programming languages. The protection profile is used to describe a class of security products that share a certain scope and can be used to solve a certain security problem. A security target on the other hand describes the security characteristics of a concrete product and how it fulfils all the requirements.

SFR as well as SAR are designed in a hierarchical structure that consists of a class at the top of the hierarchy, followed by the family and the component. The class is used to assign the SFR/SAR into predefined categories and is identified by a three-character abbreviation; see Table 1 and Table 2. Such a three-character abbreviation is also used to identify the families in the SFR and SAR. Families are a further subdivision of the category of the class to precise either the functional or the assurance requirement. Finally, the component that is identified by a number, defines for the SFR the dedicated functionality that should be provides by the TOE and for the SAR the action elements that should be performed during the evaluation.

A.2 Security functional requirements

The functional requirements in a protection profile or security target are derived from ISO/IEC 15408-2. The SFR contained in that part serve as building blocks to model the security functionality of the TOE in a semi-formal language. The fact that the security functionality of the TOE is not just described in natural language facilitates the exact definition of the functional scope of the evaluation and also serves to make different evaluations comparable. The classes in Table A.1 are used in ISO/IEC 15408-2 to categorize the functional requirements:

Table A.1 — Abbreviation of SFR

Abbreviation	Category
FAU	security audit
FCO	communication
FCS	cryptographic support
FDP	user data protection
FIA	identification and authentication
FPR	privacy
FTA	TOE access
FTP	trusted path/channels

Table A.1 *(continued)*

Abbreviation	**Category**
FRU	resource utilisation
FPT	protection of the TSF
FMT	security management

An SFR that specifies a functionality concerning the audit of events belongs accordingly to the class FAU. On the one hand, elements of this class are predefined in ISO/IEC 15408-2 and can be simply selected. On the other hand, if no sufficient predefined family is available, the author of an ST or PP may specify his/her own family. To complete the example of an SFR that belongs to the class FAU, the functionality that is responsible to generate the audit is chosen. The predefined family that describes this function has the abbreviation GEN (security audit data generation). In an ST or PP, this SFR would therefore be identified using the notation FAU_GEN.

With the same example, the generation of audit date can be possible in different level of details. These levels are also predefined in ISO/IEC 15408-2 and selected by a number that is attached to the identifier. Hence, both identifiers FAU_GEN.1 as well as FAU_GEN.2 address the generation of audit data, but in different levels of detail.

The explanations of these sections are summarized in Figure A.1.

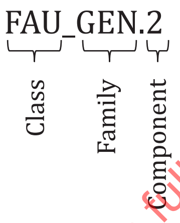

Figure A.1 — Structure of FAU_GEN.2

As already mentioned, it is important to point out that the authors of an ST or PP may define their own families and that the abbreviation should be explained in the PP or ST. This document defines some additional SFR (so-called extended SFR) to ISO/IEC 15408-2.

A.3 Security assurance requirements

The security requirements in a protection profile or security target are derived from ISO/IEC 15408-3. The SAR contained in ISO/IEC 15408-3 serve as building blocks to specify the security assurance requirements of the TOE that shall be performed during the evaluation. They are divided into the 6 categories in Table A.2.

Table A.2 — Abbreviation of SAR

Abbreviation	**Category**
ASE	security evaluation
ADV	development
AGD	guidance documents
ALC	life-cycle support
ATE	tests
AVA	vulnerability assessment

The further notation is similar to the notation used for SFR: families concretize the evaluation elements that should be performed and the number of the component defines the depth for the evaluation activities.

Annex B
(normative)

Class FPT: Protection of the TSF

B.1 Presentation attack detection (FPT_PAD)

B.1.1 FPT_PAD.1 Presentation attack detection

B.1.1.1 User application notes

FPT_PAD.1 requires that the TOE provides biometric presentation attack detection.

PAD mechanism can be affected by configurable PAD parameters. For such TSF data, only secure values shall be accepted for operational configurations so that the PAD mechanism works as intended in operational use. Therefore, FMT_MTD.3 and FMT_SMF.1 are included as dependencies of FPT_PAD.1.

B.1.1.2 Operations

B.1.1.2.1 Assignment

In FPT_PAD.1.2, the ST/PP author shall list all actions that are performed when a presentation attack is detected. The assignment shall at least contain one action.

NOTE Examples of action are message, alarm, record, and so forth, that an attack is detected.

In FPT_PAD.1.3, the ST/PP author shall list all actions that are performed when a bona fide presentation has been detected.

In FPT_PAD.1.4, the ST/PP author shall list all additional information that is delivered as feedback with presentation attack status by the PAD mechanism. Such information can be an additional score value that represents the likelihood of the presentation attack. However, the ST/PP author should understand the sensitivity of such information as a malicious user can use it to rate created PAIs. In that case, access control for such information should be considered. It may be acceptable to assign *none* here.

B.2 Biometric capture with presentation attack detection (FPT_BCP)

B.2.1 FPT_BCP.1 Check of biometric samples for capture

B.2.1.1 User application notes

In FPT_BCP.1.1, non-artificial presentation attack instrument consists of human and other natural presentation attack instruments. While human presentation attack instrument is classified into lifeless, altered, non-conformant, coerced, and conformant (see ISO/IEC 30107-1:2016, 5.2), non-conformant human presentation attack excluding mimicry should be considered (see 6.1). Such non-conformant presentation attacks include presentation with movements, rotations, or distances against the specification of the capture device (see ISO/IEC 19795-1:2006, Annex C). It also includes a presentation with a part of the biometric characteristic concealed. The TOE's decision criteria for non-artificial presentation attack instrument shall be described in the TOE design.

In FPT_BCP.1.2, artificial presentation attack instrument is a presentation attack instrument, artificially constructed as instance of a selected PAI species, which imitates biometric characteristic of the target data subject that the TOE processes. The TOE’s decision criteria for artificial presentation attack instrument shall be defined in the TOE design.

B.2.1.2 Operations — Assignment

In FPT_BCP.1.1, the ST/PP author shall specify only one biometric characteristic used for biometric capture. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric capture needs to be evaluated separately.

B.2.2 FPT_BCP.2 Biometric capture with low failure rate

Operations — Assignment

In FPT_BCP.2.1, the ST/PP author shall specify only one biometric characteristic used for biometric capture. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric capture needs to be evaluated separately.

In FPT_BCP.2.1, the definition of the FTER and FTAR depends on the enrolment and data capturing policies of the TOE. The ST author shall describe such policy in the ST.

Annex C
(normative)

Class FIA: Identification and authentication

C.1 Enrolment of biometric reference (FIA_EBR)

C.1.1 FIA_EBR.1 Check of biometric samples for enrolment

C.1.1.1 User application notes

In FIA_EBR.1.1, non-artificial presentation attack instrument consists of human and other natural presentation attack instruments. While human presentation attack instrument is classified into lifeless, altered, non-conformant, coerced, and conformant (see ISO/IEC 30107-1:2016, 5.2), non-conformant human presentation attack excluding mimicry should be considered (see 6.1). Such non-conformant presentation attacks include presentation with movements, rotations, or distances against the specification of the capture device (see ISO/IEC 19795-1:2006, Annex C). It also includes a presentation with a part concealed. The TOE's decision criteria for non-artificial presentation attack instrument shall be described in the TOE design.

In FIA_EBR.1.2, artificial presentation attack instrument is a presentation attack instrument, artificially constructed as instance of a selected PAI species, which imitates biometric characteristic of the target data subject that the TOE processes. The TOE's decision criteria for artificial presentation attack instrument shall be defined in the TOE design.

C.1.1.2 Operations — Assignment

In FIA_EBR.1.1, the ST/PP author shall specify only one biometric characteristic used for biometric enrolment. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric enrolment needs to be evaluated separately.

In FIA_EBR.1.2, the ST/PP author shall specify only one biometric characteristic used for biometric enrolment. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric enrolment needs to be evaluated separately.

C.1.2 FIA_EBR.2 Biometric enrolment with low failure to enrol rate

Operations — Assignment

In FIA_EBR.2.1, the ST/PP author shall specify only one biometric characteristic used for biometric enrolment. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric enrolment needs to be evaluated separately.

In FIA_EBR.2.1, the definition of the FTER depends on the enrolment policy of the TOE. The ST author shall describe such policy in the ST.

C.2 Biometric verification (FIA_BVR)

C.2.1 FIA_BVR.1 Biometric verification with high performance

C.2.1.1 Operations — Assignment

In FIA_BVR.1.1, the ST/PP author shall specify only one biometric characteristic used for biometric verification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric verification needs to be evaluated separately.

C.2.1.2 Operations —Selection

In FIA_BVR.1.1, the selection of the pair of error rates depends on the PP/ST.

C.2.2 FIA_BVR.2 Timing of the user authentication with biometric verification

C.2.2.1 Operations — Assignment

In FIA_BVR.2.1, the ST/PP author shall specify only one biometric characteristic used for biometric verification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric verification needs to be evaluated separately.

In FIA_BVR.2.2, the ST/PP author shall specify only one biometric characteristic used for biometric verification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric verification needs to be evaluated separately.

C.2.2.2 Operations — Selection

In FIA_BVR.2.2, the selection of the pair of error rates depends on the PP/ST.

C.2.3 FIA_BVR.3 User authentication with biometric verification before any action

C.2.3.1 Operations —Assignment

In FIA_BVR.3.1, the ST/PP author shall specify only one biometric characteristic used for biometric verification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric verification needs to be evaluated separately.

C.2.3.2 Operations — Selection

In FIA_BVR.3.1, the selection of the pair of error rates depends on the PP/ST.

C.2.4 FIA_BVR.4 Biometric verification not accepting presentation attack instruments

C.2.4.1 User application notes

In FIA_BVR.4.1, non-artificial presentation attack instrument consists of human and other natural presentation attack instruments. While human presentation attack instrument is classified into lifeless, altered, non-conformant, coerced, and conformant (see ISO/IEC 30107-1:2016, 5.2), non-conformant human presentation attack excluding mimicry should be considered (see 6.1). Such non-conformant presentation attacks include presentation with movements, rotations, or violation against the policy of the capture device (see ISO/IEC 19795-1:2006, Annex C). It also includes a presentation with a part concealed. The TOE's decision criteria for non-artificial presentation attack instrument shall be described in the TOE design.

In FIA_BVR.4.2, artificial presentation attack instrument is a presentation attack instrument, artificially constructed as instance of a selected PAI species, which imitates biometric characteristic of the target data subject that the TOE processes. The TOE's decision criteria for artificial presentation attack instrument shall be defined in the TOE design.

C.2.4.2 Operations — Assignment

In FIA_BVR.4.1, the ST/PP author shall specify only one biometric characteristic used for biometric verification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric verification needs to be evaluated separately.

In FIA_BVR.4.2, the ST/PP author shall specify only one biometric characteristic used for biometric verification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric verification needs to be evaluated separately.

C.3 Biometric identification (FIA_BID)

C.3.1 FIA_BID.1 Biometric identification with high performance

C.3.1.1 Operations — Assignment

In FIA_BID.1.1, the ST/PP author shall specify only one biometric characteristic used for biometric identification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric identification needs to be evaluated separately.

C.3.1.2 Operations —Selection

In FIA_BID.1.1, the selection of the pair of error rates depends on the PP/ST.

C.3.2 FIA_BID.2 Timing of the biometric identification

C.3.2.1 Operations — Assignment

In FIA_BID.2.1, the ST/PP author shall specify only one biometric characteristic used for biometric identification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric identification needs to be evaluated separately.

In FIA_BID.2.2, the ST/PP author shall specify only one biometric characteristic used for biometric identification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric identification needs to be evaluated separately.

C.3.2.2 Operations — Selection

In FIA_BID.2.2, the selection of the pair of error rates depends on the PP/ST.

C.3.3 FIA_BID.3 Biometric identification before any action

C.3.3.1 Operations — Assignment

In FIA_BID.3.1, the ST/PP author shall specify only one biometric characteristic used for biometric identification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric identification needs to be evaluated separately.

C.3.3.2 Operations — Selection

In FIA_BID.3.1, the selection of the pair of error rates depends on the PP/ST.

C.3.4 FIA_BID.4 Biometric identification not accepting presentation attack instruments

C.3.4.1 User application notes

In FIA_BID.4.1, non-artificial presentation attack instrument consists of human and other natural presentation attack instruments. While human presentation attack instrument is classified into lifeless, altered, non-conformant, coerced, and conformant (see ISO/IEC 30107-1:2016, 5.2), non-conformant human presentation attack excluding mimicry should be considered (see 6.1). Such non-conformant presentation attacks include presentation with movements, rotations, or violation against the policy of the capture device (see ISO/IEC 19795-1:2006, Annex C). It also includes a presentation with a part concealed. The TOE's decision criteria for non-artificial presentation attack instrument shall be described in the TOE design.

In FIA_BID.4.2, artificial presentation attack instrument is a presentation attack instrument artificially constructed as instance of a selected PAI species, which imitates biometric characteristic of the target data subject that the TOE processes. The TOE's decision criteria for artificial presentation attack instrument shall be defined in the TOE design.

C.3.4.2 Operations — Assignment

In FIA_BID.4.1, the ST/PP author shall specify only one biometric characteristic used for biometric identification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric identification needs to be evaluated separately.

In FIA_BID.4.2, the ST/PP author shall specify only one biometric characteristic used for biometric identification. If the ST/PP author specify multiple biometric characteristics, the ST/PP author shall use iteration operation and each biometric identification needs to be evaluated separately.

Annex D
(informative)

Background information on supplementary activities for PAD evaluation

D.1 Class APE: Protection Profile evaluation/Class ASE: Security Target evaluation

D.1.1 APE_INT PP introduction/ASE_INT ST introduction

A ST/PP should never claim maximum acceptable error rates for PAD (e.g. APCER, BPCER as defined in ISO/IEC 30107-3), as these rates do not have to be published in the ST/PP after the evaluation. Adequateness of the PAD mechanism is determined during testing (ATE) and vulnerability assessment (AVA) in the context of the used assurance level.

The overall statement concerning the PAD mechanism should be that the system is generally able to detect presentation attacks assuming the described operational environment and a specific attack potential (as defined by the use of a specific component of AVA_VAN). Part of the testing activity is to determine whether the produced error rates are sufficient to satisfy the claimed assurance level under the assumptions on the operational environment.

The introduction of the ST should clearly identify the biometric characteristics (e.g. fingerprints) that the PAD subsystem can be used for. This information is very important for potential customers looking for a certified TOE with PAD mechanism as they usually are after protecting a technology basing on a specific biometric characteristic.

The introduction should also include information about the protected biometric system and should identify the biometric functionality (e.g. enrolment, verification, identification) and, where known, the intended use of the biometric system which are of specific importance. for the evaluator. This information is used to inform the evaluation with regard to performance testing requirements, vulnerability analysis and the calculation of attack potential.

As demanded by the requirements of the ISO/IEC 15408 series, the ST should describe the hardware components comprising the TOE. The ST should provide the overview of the PAD mechanism including a description of its operation.

D.1.2 APE_SPD Security problem definition/ASE_SPD Security problem definition

The ST/PP should describe organizational security policies for personal data privacy protection, including measures for protecting the privacy of the biometric data and particularly sensitive data such as data which can reveal health information about users.

NOTE Where a PP cannot include detailed descriptions because of its generic nature, the descriptions are provided in the ST.

D.2 Class ADV: Development

D.2.1 ADV_ARC Security architecture

In the security architecture documentation, the developer should describe how the capture process of the biometric data and the process for PAD work together. There are several possibilities. The PAD subsystem can be wholly integrated into a distinct biometric capture subsystem. Alternatively, it can be distributed across one of more subsystems (e.g. the biometric capture subsystem and the signal processing subsystem)

The developer should describe how it is ensured that the biometric characteristic which is used for capturing the biometric sample is the same one which is used for PAD. Using this information, the evaluator should gain confidence that it is not possible to bypass the PAD mechanism. For example, in a fingerprint recognition system, if the PAD mechanism precedes the fingerprint sample capture, it can be possible to mount a successful attack on the system by presenting a live finger to satisfy the PAD test followed by an artefact to provide the biometric recognition sample. More information about this kind of vulnerability is provided in E.2.

D.2.2 ADV_FSP Functional specification

The functional specification should particularly describe the TSFIs to the PAD mechanism.

If more than one mechanism is used to determine whether a presentation is an attack presentation or not, then each mechanism should be described using either separate interfaces, separate sub-interfaces, or separate parameters for a TSFI.

If a PAD mechanism for example uses a temperature sensor and a capacitive sensor for its PAD, the developer should describe an interface which is decomposed into a sub-interface for the temperature sensor and a sub-interface for the capacitive sensor.

This should be done in order to give the evaluator a clear understanding of each mechanism and of the different physical aspects of the presentation which the mechanisms are based on. This information is necessary in the context of vulnerability assessment since an attacker can use every channel/mechanism available (or a combination of them) to tamper with the TSF.

The developer should also consider interface parameters for sensors. For example, such parameters can be the temperature or the moisture of a presented biometric characteristic, the intensity of ambient light, or the pressure that is applied to the capture device by the finger.

During the evaluation of the functional specification, the evaluator should consider whether the TSFI provide feedback on the decision of the PAD mechanism to the user. Under certain conditions, an attacker can use such feedback to perform hill-climbing attacks on the PAD mechanism. For instance, if a TSFI provide score values representing the probability that a presention is an attack, attackers can use this value to rate and improve PAIs for more sophisticated attacks.

If sensor devices used for PAD mechanism are part of the TOE, the developer should describe how the TSFI to the sensor is intended to be used by users. Specifically, the developer should describe the process of presenting the biometric characteristic to the sensor. Note that this information can also be part of the guidance documentation in which case the guidance may be referenced by the FSP.

D.2.3 ADV_IMP Implementation representation

A PAD mechanism may refer to some kind of database in order to determine whether a presention is an attack or not (e.g. when presentation attacks are detected using pattern matching). In this case, the database is security relevant for the functionality of the PAD. Therefore, it should also be provided to the evaluator as a part of the implementation representation.

Such a database may be a highly dynamic part of a PAD mechanism as the database is updated once new kinds of PAI appear. The developer should therefore decide to provide dedicated version information for this database and to separate it from the rest of the implementation representation (e.g. by assigning a dedicated subsystem or module to it). Such a separation of the dynamic aspects of this kind of a database can facilitate re-evaluations of the TOE if the database is the only part that is being updated.

However, it shall be clearly mentioned that a certification of a TOE is only valid for one version of the database (unless more than one configuration of a TOE would be evaluated).

D.2.4 ADV_TDS TOE design

In the TOE design, the developer provides further information on the TSF by describing TOE subsystems and modules. For systems that implement PAD, the TOE design should describe the presentation attack evidence that is examined as well as the mechanisms that are used to check the evidence to detect presentation attacks. Examples for presentation attack evidence for fingerprint are:

- finger moisture;
- electrical capacity of finger;
- finger temperature;
- blood circulation in finger;
- blood oxygen in finger;
- pulse;
- optical density.

Examples for mechanisms to check the presentation attack evidence are:

- capacity measuring;
- spectral analysis;
- pulse oximetry for the measurement of blood oxygen;
- thermometer;
- ultrasonic pulse-echo (ultrasonography).

PAD mechanisms are typically based on the detection of artificial PAIs or on sensing the liveness of a presentation or a combination of both. Artificial PAIs detection attempts to distinguish artificial PAIs presentations from natural biometric characteristic presentations by measurement of physical properties of the presentation (which can include liveness). Liveness detection attempts to identify living biometric characteristics, for example by measuring blood oxygen saturation or pulse. This information is useful for the evaluator when trying to identify potential attacks on the TOE during vulnerability assessment (see ISO/IEC 19989-3). The developer should also describe the underlying theoretical background for the used mechanisms so that the evaluator is able to determine its potency for PAD. In particular, the developer should describe how the signals from the sensors are processed and transformed into presentation attack evidence.

The TOE design should reveal the interactions between PAD mechanism and capture functionality. Detailed information on the implementation of the TOE PAD mechanisms is important for the evaluator to help them to identify areas of potential vulnerability and to inform the vulnerability assessment process.

If a biometric verification system uses the TOE of PAD subsystem and allows users to repeat authentication attempts when the PAD detected an attack presentation, then this should be described in the TDS. The number of retries is critical for defining appropriate maximum error rates in ATE. The environment that the TOE is supposed to work in is also relevant as the retries can also be limited by the operator surveying the TOE operation.

During the review, the evaluator should consider which PAI materials can possibly be detected and which can not be detected by the PAD mechanism. This also gives hints for the vulnerability analysis (see ISO/IEC 19989-3). For example, if the PAD uses a capacitive sensor to measure the capacity of a finger, the evaluator can try to use a mixture of wood glue and graphite powder to copy the electrical behaviour of a finger