見出し 1STD Version 2.8l C:\Users\YAMADA Asahiko\Documents\JTC 1\SC 27\WG 3\19989\3パート期\Part 1\06 DIS\ISO-IEC\_19989-1\_(E).docx   4 2   63        ISO/IEC  19989-1:2020(E)    40見出し 2 0  ‑ISO/IEC 19989‑1 ISO/IEC J© ISO/IEC 2020 – All rights reservedISO/IEC DIS 19989-1Security techniques — Criteria and methodology for security evaluation of biometric systemsPart 1: FrameworkSecurity techniques — Criteria and methodology for security evaluation of biometric systems — Part 1: FrameworkÉlément introductif — Élément central — Partie 1: Titre de la partieInternational Standard2020  (40) Enquiry127Information technologyIT security techniques3DIN E2019-05-10DRAFT INTERNATIONAL STANDARD  ISO/IECISO/IEC 19989ISO/IEC JTC 1/SC 27 N19512

Date: 202x-xx-xx

ISO/IEC 19989-1:202x(E)

ISO/IEC JTC 1/SC 27/WG 3

Secretariat: DIN

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*

COPYRIGHT PROTECTED DOCUMENT

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO’s member body in the country of the requester.

ISO copyright office

Ch. de Blandonnet 8 • CP 401

CH-1214 Vernier, Geneva, Switzerland

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

copyright@iso.org

[www.iso.org](http://www.iso.org)

Contents Page

[Foreword 13](#_Toc172671502)

[Introduction 15](#_Toc172671503)

[1 Scope 1](#_Toc172671504)

[2 Normative references 1](#_Toc172671505)

[3 Terms and definitions 2](#_Toc172671506)

[4 Symbols and abbreviated terms 4](#_Toc172671507)

[5 General remarks 4](#_Toc172671508)

[6 Vulnerabilities in biometric systems and security evaluation 5](#_Toc172671509)

[6.1 Categorization of common vulnerabilities of biometric systems 5](#_Toc172671510)

[6.2 Biometric system and presentation attack detection 8](#_Toc172671511)

[6.3 Categorization of TOEs in relation to the type of evaluation 10](#_Toc172671512)

[6.3.1 Biometric recognition performance evaluation 10](#_Toc172671513)

[6.3.2 PAD evaluation 11](#_Toc172671514)

[7 Extended security functional components to Class FPT: Protection of the TSF 11](#_Toc172671515)

[7.1 General 11](#_Toc172671516)

[7.2 Presentation attack detection (FPT\_PAD) 11](#_Toc172671517)

[7.2.1 Family behaviour 11](#_Toc172671518)

[7.2.2 Component levelling 12](#_Toc172671519)

[7.2.3 Management of FPT\_PAD.1 12](#_Toc172671520)

[7.2.4 Audit of FPT\_PAD.1 12](#_Toc172671521)

[7.2.5 FPT\_PAD.1 Presentation attack detection 12](#_Toc172671522)

[7.3 Biometric capture with presentation attack detection (FPT\_BCP) 13](#_Toc172671523)

[7.3.1 Family behaviour 13](#_Toc172671524)

[7.3.2 Component levelling 13](#_Toc172671525)

[7.3.3 Management of FPT\_BCP.1 13](#_Toc172671526)

[7.3.4 Management of FPT\_BCP.2 13](#_Toc172671527)

[7.3.5 Audit of FPT\_BCP.1 13](#_Toc172671528)

[7.3.6 Audit of FPT\_BCP.2 14](#_Toc172671529)

[7.3.7 FPT\_BCP.1 Check of biometric samples for capture 14](#_Toc172671530)

[7.3.8 FPT\_BCP.2 Biometric capture with low failure rate 14](#_Toc172671531)

[8 Extended security functional components to Class FIA: Identification and authentication 15](#_Toc172671532)

[8.1 General 15](#_Toc172671533)

[8.2 Enrolment of biometric reference (FIA\_EBR) 15](#_Toc172671534)

[8.2.1 Family behaviour 15](#_Toc172671535)

[8.2.2 Component levelling 15](#_Toc172671536)

[8.2.3 Management of FIA\_EBR.1 15](#_Toc172671537)

[8.2.4 Management of FIA\_EBR.2 16](#_Toc172671538)

[8.2.5 Audit of FIA\_EBR.1 16](#_Toc172671539)

[8.2.6 Audit of FIA\_EBR.2 16](#_Toc172671540)

[8.2.7 FIA\_EBR.1 Check of biometric samples for enrolment 16](#_Toc172671541)

[8.2.8 FIA\_EBR.2 Biometric enrolment with low failure to enrol rate 16](#_Toc172671542)

[8.3 Biometric verification (FIA\_BVR) 17](#_Toc172671543)

[8.3.1 Family behaviour 17](#_Toc172671544)

[8.3.2 Component levelling 17](#_Toc172671545)

[8.3.3 Management of FIA\_BVR.1 17](#_Toc172671546)

[8.3.4 Management of FIA\_BVR.2 17](#_Toc172671547)

[8.3.5 Management of FIA\_BVR.3 17](#_Toc172671548)

[8.3.6 Management of FIA\_BVR.4 18](#_Toc172671549)

[8.3.7 Audit of FIA\_BVR.1 18](#_Toc172671550)

[8.3.8 Audit of FIA\_BVR.2 18](#_Toc172671551)

[8.3.9 Audit of FIA\_BVR.3 18](#_Toc172671552)

[8.3.10 Audit of FIA\_BVR.4 18](#_Toc172671553)

[8.3.11 FIA\_BVR.1 Biometric verification with high performance 19](#_Toc172671554)

[8.3.12 FIA\_BVR.2 Timing of user authentication with biometric verification 19](#_Toc172671555)

[8.3.13 FIA\_BVR.3 User authentication with biometric verification before any action 19](#_Toc172671556)

[8.3.14 FIA\_BVR.4 Biometric verification not accepting presentation attack instruments 20](#_Toc172671557)

[8.4 Biometric identification (FIA\_BID) 20](#_Toc172671558)

[8.4.1 Family behaviour 20](#_Toc172671559)

[8.4.2 Component levelling 20](#_Toc172671560)

[8.4.3 Management of FIA\_BID.1 21](#_Toc172671561)

[8.4.4 Management of FIA\_BID.2 21](#_Toc172671562)

[8.4.5 Management of FIA\_BID.3 21](#_Toc172671563)

[8.4.6 Management of FIA\_BID.4 21](#_Toc172671564)

[8.4.7 Audit of FIA\_BID.1 21](#_Toc172671565)

[8.4.8 Audit of FIA\_BID.2 21](#_Toc172671566)

[8.4.9 Audit of FIA\_BID.3 21](#_Toc172671567)

[8.4.10 Audit of FIA\_BID.4 22](#_Toc172671568)

[8.4.11 FIA\_BID.1 Biometric identification with high performance 22](#_Toc172671569)

[8.4.12 FIA\_BID.2 Timing of biometric identification 22](#_Toc172671570)

[8.4.13 FIA\_BID.3 Biometric identification before any action 23](#_Toc172671571)

[8.4.14 FIA\_BID.4 Biometric identification not accepting presentation attack instruments 23](#_Toc172671572)

[9 Supplementary activities to ISO/IEC 18045 on Class APE: Protection Profile evaluation 23](#_Toc172671573)

[10 Supplementary activities to ISO/IEC 18045 on Class ASE: Security Target evaluation 24](#_Toc172671574)

[11 Supplementary activities to ISO/IEC 18045 on Class ADV: Development 25](#_Toc172671575)

[11.1 Supplementary activities to security architecture ADV\_ARC 25](#_Toc172671576)

[11.2 Supplementary activities to functional specification ADV\_FSP 25](#_Toc172671577)

[11.2.1 Supplementary activities to evaluation of sub-activity ADV\_FSP.1 25](#_Toc172671578)

[11.2.2 Supplementary activities to evaluation of sub-activity ADV\_FSP.2 25](#_Toc172671579)

[11.2.3 Supplementary activities to Evaluation of sub-activity ADV\_FSP.3 26](#_Toc172671580)

[11.2.4 Supplementary activities to Evaluation of sub-activity ADV\_FSP.4 27](#_Toc172671581)

[11.3 Supplementary activities to TOE design ADV\_TDS 28](#_Toc172671582)

[11.3.1 Supplementary activities to evaluation of sub-activity ADV\_TDS.1 28](#_Toc172671583)

[11.3.2 Supplementary activities to evaluation of sub-activity ADV\_TDS.2 29](#_Toc172671584)

[11.3.3 Supplementary activities to evaluation of sub-activity ADV\_TDS.3 29](#_Toc172671585)

[12 Supplementary activities to ISO/IEC 18045 on Class AGD: Guidance documents 30](#_Toc172671586)

[12.1 Supplementary activities to operational user guidance AGD\_OPE 30](#_Toc172671587)

[12.2 Supplementary activities to preparative procedures AGD\_PRE 31](#_Toc172671588)

[13 Supplementary activities to ISO/IEC 18045 on Class ALC: Life-cycle support 31](#_Toc172671589)

[13.1 Supplementary activities to CM support ALC\_CMS 31](#_Toc172671590)

[13.2 Supplementary activities to Delivery ALC\_DEL 32](#_Toc172671591)

[13.3 Supplementary activities to flaw remediation ALC\_FLR 32](#_Toc172671592)

[14 Supplementary activities to ISO/IEC 18045 on Class ATE: Tests 32](#_Toc172671593)

[14.1 Supplementary activities to functional tests ATE\_FUN 32](#_Toc172671594)

[14.2 Supplementary activities to independent testing ATE\_IND 33](#_Toc172671595)

[14.2.1 General 33](#_Toc172671596)

[14.2.2 Supplementary activities to evaluation of sub-activity ATE\_IND.1 33](#_Toc172671597)

[14.2.3 Supplementary activities to Evaluation of sub-activity ATE\_IND.2 34](#_Toc172671598)

[15 Supplementary activities to ISO/IEC 18045 on Class AVA: Vulnerability assessment 36](#_Toc172671599)

[15.1 General 36](#_Toc172671600)

[15.2 Supplementary activities to vulnerability analysis AVA\_VAN 36](#_Toc172671601)

[15.2.1 Supplementary activities to evaluation of sub-activity AVA\_VAN.2 36](#_Toc172671602)

[15.2.2 Supplementary activities to evaluation of sub-activity AVA\_VAN.3 37](#_Toc172671603)

[15.2.3 Supplementary activities to evaluation of sub-activity AVA\_VAN.4 38](#_Toc172671604)

[Annex A (informative) Introduction to the basic concepts of ISO/IEC 15408 40](#_Toc172671605)

[A.1 General 40](#_Toc172671606)

[A.2 Security functional requirements 40](#_Toc172671607)

[A.3 Security assurance requirements 41](#_Toc172671608)

[Annex B (normative) Class FPT: Protection of the TSF 43](#_Toc172671609)

[B.1 Presentation attack detection (FPT\_PAD) 43](#_Toc172671610)

[B.1.1 FPT\_PAD.1 Presentation attack detection 43](#_Toc172671611)

[B.1.1.1 User application notes 43](#_Toc172671612)

[B.1.1.2 Operations 43](#_Toc172671613)

[B.1.1.2.1 Assignment 43](#_Toc172671614)

[B.2 Biometric capture with presentation attack detection (FPT\_BCP) 43](#_Toc172671615)

[B.2.1 FPT\_BCP.1 Check of biometric samples for capture 43](#_Toc172671616)

[B.2.1.1 User application notes 43](#_Toc172671617)

[B.2.1.2 Operations — Assignment 44](#_Toc172671618)

[B.2.2 FPT\_BCP.2 Biometric capture with low failure rate 44](#_Toc172671619)

[Annex C (normative) Class FIA: Identification and authentication 45](#_Toc172671620)

[C.1 Enrolment of biometric reference (FIA\_EBR) 45](#_Toc172671621)

[C.1.1 FIA\_EBR.1 Check of biometric samples for enrolment 45](#_Toc172671622)

[C.1.1.1 User application notes 45](#_Toc172671623)

[C.1.1.2 Operations — Assignment 45](#_Toc172671624)

[C.1.2 FIA\_EBR.2 Biometric enrolment with low failure to enrol rate 45](#_Toc172671625)

[C.2 Biometric verification (FIA\_BVR) 45](#_Toc172671626)

[C.2.1 FIA\_BVR.1 Biometric verification with high performance 45](#_Toc172671627)

[C.2.1.1 Operations — Assignment 45](#_Toc172671628)

[C.2.1.2 Operations —Selection 46](#_Toc172671629)

[C.2.2 FIA\_BVR.2 Timing of user authentication with biometric verification 46](#_Toc172671630)

[C.2.2.1 Operations — Assignment 46](#_Toc172671631)

[C.2.2.2 Operations — Selection 46](#_Toc172671632)

[C.2.3 FIA\_BVR.3 User authentication with biometric verification before any action 46](#_Toc172671633)

[C.2.3.1 Operations —Assignment 46](#_Toc172671634)

[C.2.3.2 Operations — Selection 46](#_Toc172671635)

[C.2.4 FIA\_BVR.4 Biometric verification not accepting presentation attack instruments 46](#_Toc172671636)

[C.2.4.1 User application notes 46](#_Toc172671637)

[C.2.4.2 Operations — Assignment 46](#_Toc172671638)

[C.3 Biometric identification (FIA\_BID) 47](#_Toc172671639)

[C.3.1 FIA\_BID.1 Biometric identification with high performance 47](#_Toc172671640)

[C.3.1.1 Operations — Assignment 47](#_Toc172671641)

[C.3.1.2 Operations —Selection 47](#_Toc172671642)

[C.3.2 FIA\_BID.2 Timing of biometric identification 47](#_Toc172671643)

[C.3.2.1 Operations — Assignment 47](#_Toc172671644)

[C.3.2.2 Operations — Selection 47](#_Toc172671645)

[C.3.3 FIA\_BID.3 Biometric identification before any action 47](#_Toc172671646)

[C.3.3.1 Operations — Assignment 47](#_Toc172671647)

[C.3.3.2 Operations — Selection 47](#_Toc172671648)

[C.3.4 FIA\_BID.4 Biometric identification not accepting presentation attack instruments 47](#_Toc172671649)

[C.3.4.1 User application notes 47](#_Toc172671650)

[C.3.4.2 Operations — Assignment 48](#_Toc172671651)

[Annex D (informative) Background information on supplementary activities for PAD evaluation 49](#_Toc172671652)

[D.1 Class APE: Protection Profile evaluation/Class ASE: Security Target evaluation 49](#_Toc172671653)

[D.1.1 APE\_INT PP introduction/ASE\_INT ST introduction 49](#_Toc172671654)

[D.1.2 APE\_SPD Security problem definition/ASE\_SPD Security problem definition 49](#_Toc172671655)

[D.2 Class ADV: Development 49](#_Toc172671656)

[D.2.1 ADV\_ARC Security architecture 49](#_Toc172671657)

[D.2.2 ADV\_FSP Functional specification 50](#_Toc172671658)

[D.2.3 ADV\_IMP Implementation representation 50](#_Toc172671659)

[D.2.4 ADV\_TDS TOE design 51](#_Toc172671660)

[D.3 Class AGD: Guidance documents 52](#_Toc172671661)

[D.3.1 AGD\_OPE Operational user guidance 52](#_Toc172671662)

[D.3.2 AGD\_PRE Preparative procedures 52](#_Toc172671663)

[D.4 Class ALC: Life-cycle support 53](#_Toc172671664)

[D.4.1 ALC\_CMS CM scope 53](#_Toc172671665)

[D.4.2 ALC\_DEL Delivery 53](#_Toc172671666)

[D.4.3 ALC\_FLR Flaw remediation 53](#_Toc172671667)

[D.4.4 ALC\_TAT Tools and techniques 54](#_Toc172671668)

[D.5 Class ATE: Tests 54](#_Toc172671669)

[D.5.1 ATE\_FUN Functional tests 54](#_Toc172671670)

[D.5.2 ATE\_IND Independent testing 54](#_Toc172671671)

[D.6 Class AVA: Vulnerability assessment 55](#_Toc172671672)

[D.6.1 AVA\_VAN Vulnerability analysis 55](#_Toc172671673)

[Annex E (informative) Other general vulnerabilities 56](#_Toc172671674)

[E.1 General 56](#_Toc172671675)

[E.2 Two-channel attacks 56](#_Toc172671676)

[E.3 Feedback provided by TOEs 56](#_Toc172671677)

[Annex F (normative) Attack potential and TOE resistance 58](#_Toc172671678)

[F.1 Calculating attack potential 58](#_Toc172671679)

[F.1.1 General 58](#_Toc172671680)

[F.1.2 Identification and exploitation of attacks 58](#_Toc172671681)

[F.1.2.1 Identification of attacks 58](#_Toc172671682)

[F.1.2.2 Exploitation of attacks 58](#_Toc172671683)

[F.1.3 Factors to be considered 58](#_Toc172671684)

[F.1.4 Calculation of attack potential 62](#_Toc172671685)

[F.1.5 Rating of vulnerabilities and TOE resistance 64](#_Toc172671686)

[Annex G (normative) Adapted Versions of Attack potential 65](#_Toc172671687)

[G.1 Calculating attack potential for specific use cases 65](#_Toc172671688)

[G.1.1 Mobile fingerprint verification 65](#_Toc172671689)

[G.1.1.1 Choosing the level 65](#_Toc172671690)

[G.1.1.2 Key factors for classification 66](#_Toc172671691)

[G.1.1.3 Prefixed attack potential table for each level 67](#_Toc172671692)

[G.1.2 Online scenarios 69](#_Toc172671693)

[G.1.2.1 Use of the TOE 69](#_Toc172671694)

[G.1.2.2 Replicability 69](#_Toc172671695)

[G.1.3 Digital attacks 70](#_Toc172671696)

[G.1.3.1 Elapsed time 70](#_Toc172671697)

[G.1.3.2 Expertise 70](#_Toc172671698)

[G.2 Calculating attack potential for TOEs with low level of resistance 70](#_Toc172671699)

[G.3 Mapping of levels of assurance with EU framework (added here as per request from some experts but feasibility of this discussion has to be confirmed/discussed) 71](#_Toc172671700)

[Annex H (informative) Examples of attack potential 72](#_Toc172671701)

[H.1 Example 1 72](#_Toc172671702)

[H.2 Example 2 72](#_Toc172671703)

[Bibliography 74](#_Toc172671704)

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](https://www.iso.org/directives-and-policies.html)).

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](https://www.iso.org/iso-standards-and-patents.html)) or the IEC list of patent declarations received (see [http://patents.iec.ch](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](https://www.iso.org/foreword-supplementary-information.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](https://www.iso.org/members.html).

Editor’s note: Revision statement to be added

Editor’s NOTE: as per the revision intent circulated in April 2024 WG3 meeting, comments and contributions from experts are invited on

* A revision of Annex F “attack potential and TOE resistance”, to update some of the names of the criteria and to update the calculation table and the corresponding threshold in order to better cope with recent attack scenarios (injection attacks, deepfakes, masterprints, …)
* A discussion of possible new criteria (like replicability) to reflect some newer use cases like biometrics deployed on widely available devices.
* A discussion of possible division of attack potential table into a common part that should be applied to all attack scenarios and attack specific part that should be applied to a specific attack scenario.
* A discussion of possible improvement of attack rating considering the result of past evaluations.
* The creation of a new annex to include examples of use cases and attack scenario to guide the reader on ways to instantiate Annex F when assessing some attack potentials.
* Improvement and correction of other clauses and annexes of the document where needed

This version highlights the modifications made (track changes) from the 2020 published version. Early contributions related to Annex F have been included. Some technical comments received in FDIS ballot and pre-publication version of 2020 edition were included as well when deemed easily feasible by editors.

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.

Note that the document hierarchical structures and expressions in Clause 7, 8, Annex B, and C have changed from those corresponding in ISO/IEC 15408-2:2008 as the editorial policy has changed.

Security techniques — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework

# 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.

# 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

Editor’s note: discussion/contributions welcomed to update to latest versions of 15408 and 18045.

# 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).

# 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 |

# 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.

# Vulnerabilities in biometric systems and security evaluation

## 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.

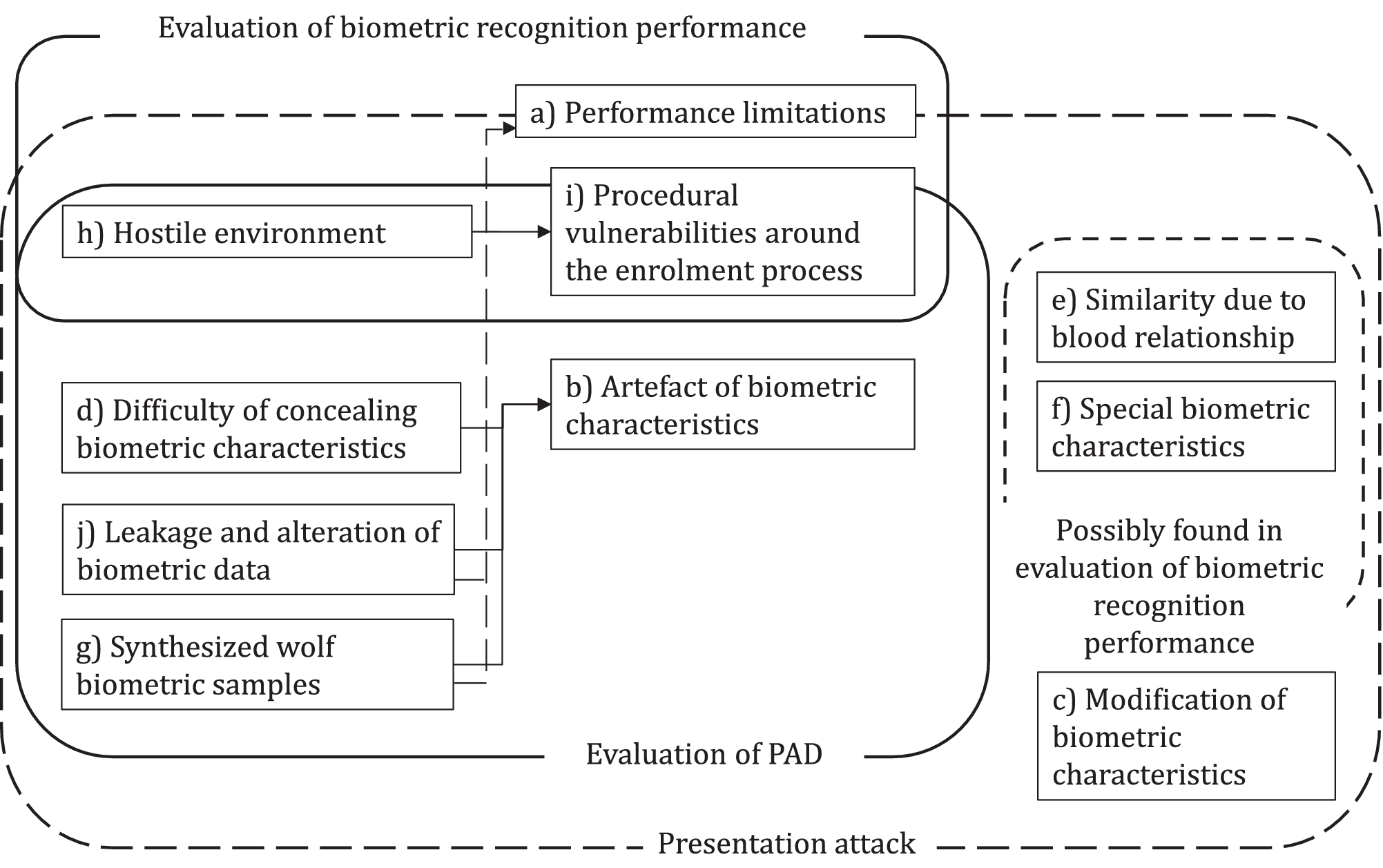


Figure 1 — The relation of vulnerability factors in biometric systems

Editor’s note: Figure 1 to be adapted in order to clearly display the relation between different types of evaluation and vulnerability factors, using different types of line (eg. long dotted line, short dotted line, solid line) to identify Presentation Attack，Evaluation of PAD，Evaluation of biometric recognition performance.

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.

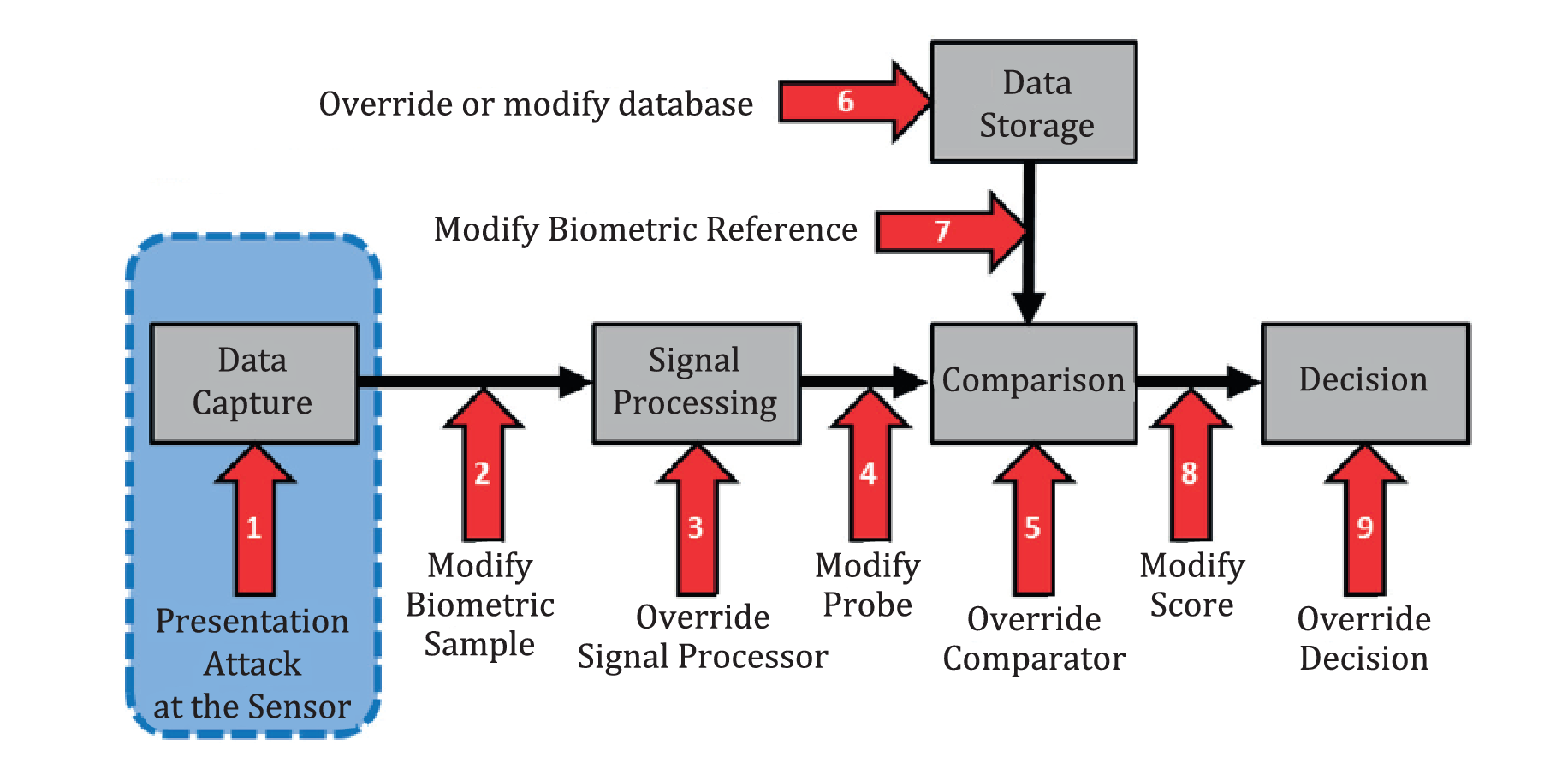


Figure 2 — Examples of points of attack in a biometric system (from ISO/IEC 30107-1)

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.

## 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.

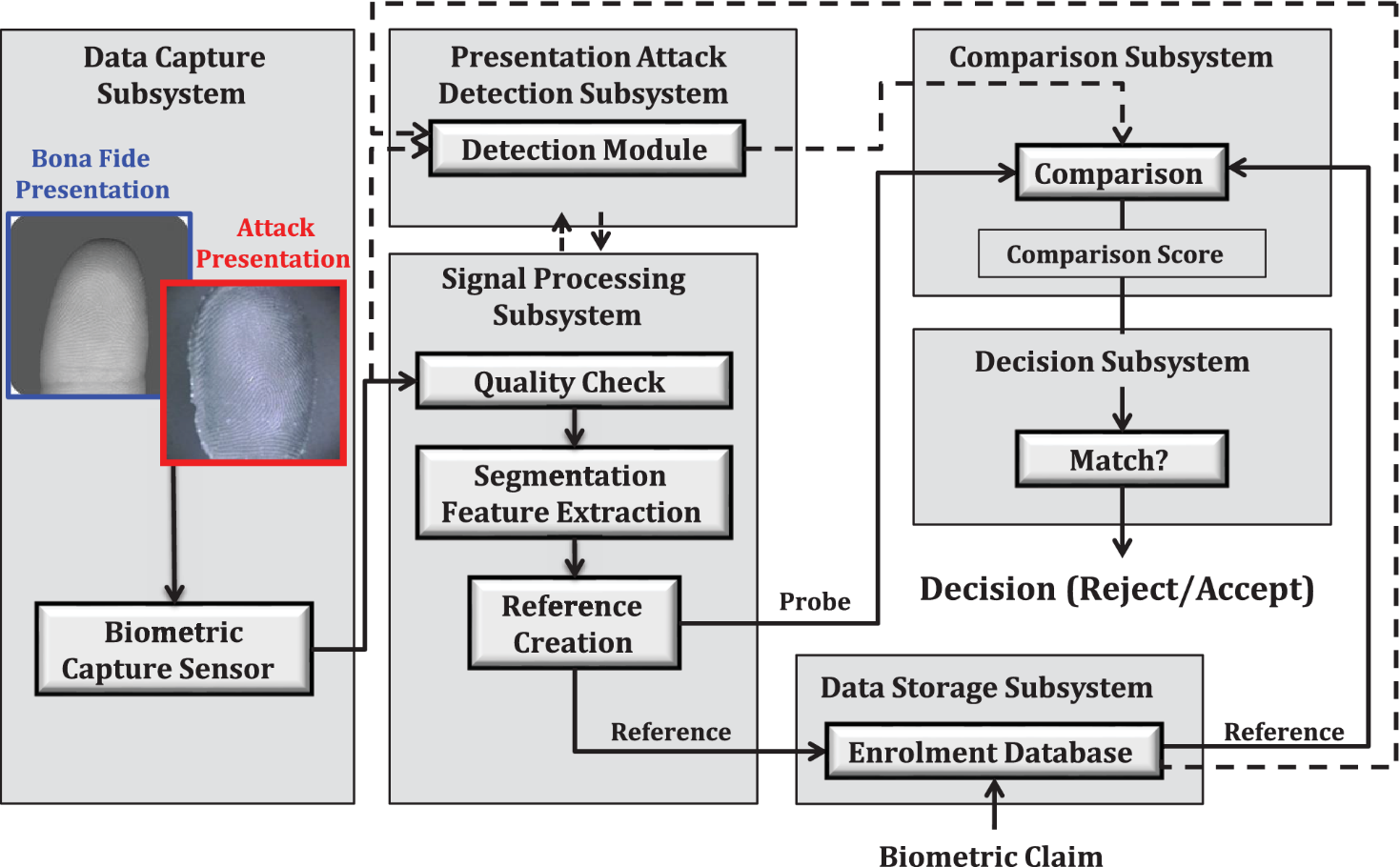


Figure 3 — General biometric framework incorporating PAD subsystem (conceptual representation)

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".

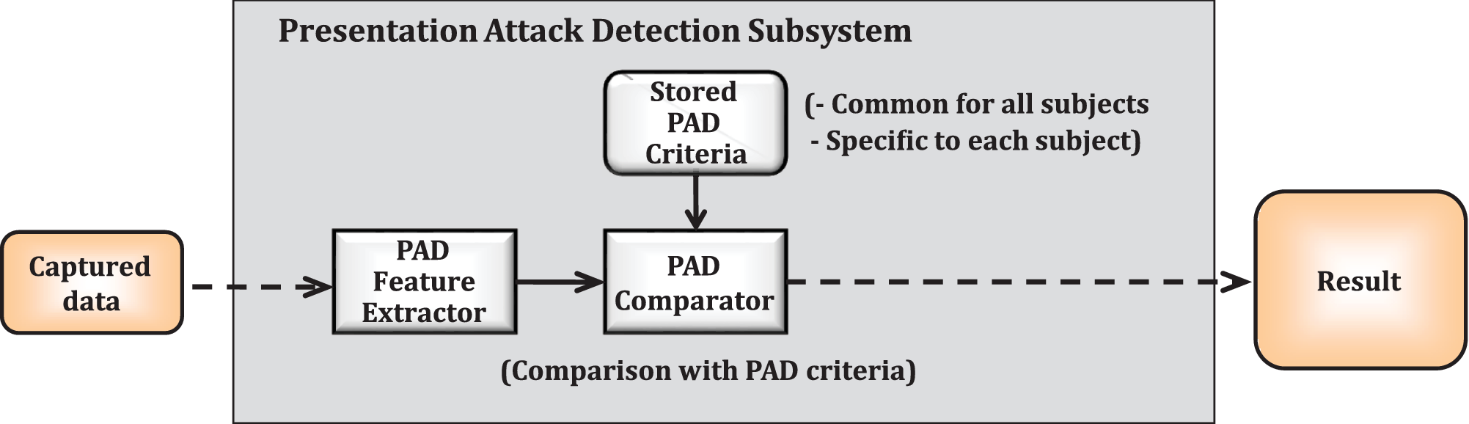


Figure 4 — Components in a general PAD subsystem

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).

## Categorization of TOEs in relation to the type of evaluation

### 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 evaluation for example would usually only comprise the software for comparison, with a dependency that requires the software to be executed 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.

### 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.

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

## 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).

## Presentation attack detection (FPT\_PAD)

### 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.

### Component levelling

Figure 5 shows the structure of this family.



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.

### 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.

### 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.

### 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.

## Biometric capture with presentation attack detection (FPT\_BCP)

### 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.

### Component levelling

Figure 6 shows the structure of this family.



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.

Editor’s note: consider better wording for FPT\_BCP.2 biometric capture with low failure rate

### 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.

### 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.

### 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).

### 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.

### 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.

### 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.

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

## 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.

## Enrolment of biometric reference (FIA\_EBR)

### 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.

### Component levelling

Figure 7 shows the structure of this family.

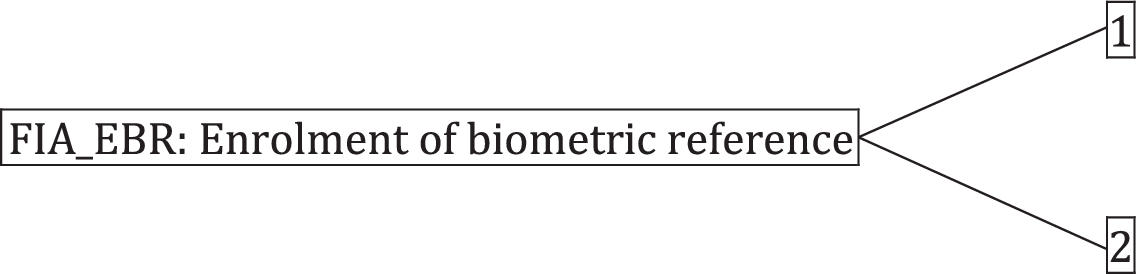


Figure 7 — FIA\_EBR Enrolment of biometric reference family

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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

## Biometric verification (FIA\_BVR)

### 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.

### Component levelling

Figure 8 shows the structure of this family.

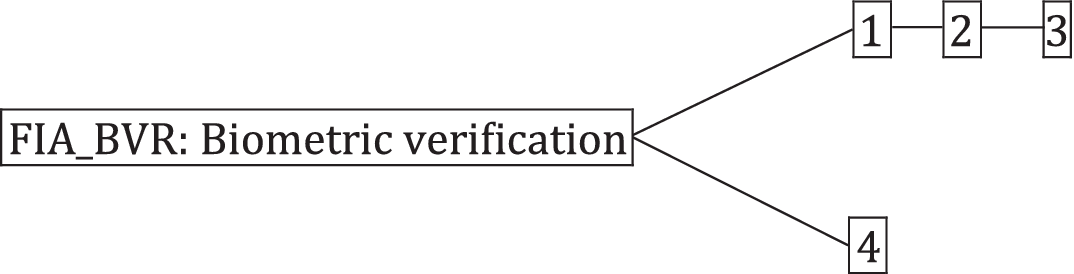


Figure 8 — FIA\_BVR Biometric verification

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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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 characteristi*c] 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.

### FIA\_BVR.2 Timing of user authentication with biometric verification

|  |  |
| --- | --- |
| Hierarchical to: | FIA\_BVR.1 biometric verification with high performance |
| 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.

### FIA\_BVR.3 User authentication with biometric verification before any action

|  |  |
| --- | --- |
| Hierarchical to: | FIA\_BVR.2 timing of 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.

### 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.

## Biometric identification (FIA\_BID)

### 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.

### Component levelling

Figure 9 shows the structure of this family.

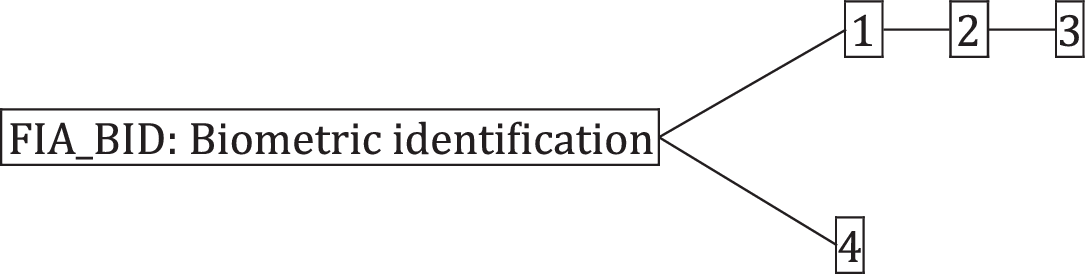


Figure 9 — FIA\_BID Biometric identification

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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### FIA\_BID.2 Timing of biometric identification

|  |  |
| --- | --- |
| Hierarchical to: | FIA\_BID.1 biometric identification with high performance |
| 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.

### FIA\_BID.3 Biometric identification before any action

|  |  |
| --- | --- |
| Hierarchical to: | FIA\_BID.2 timing of 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.

### 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.

# 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.

# 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 |

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

## 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) |

## Supplementary activities to functional specification ADV\_FSP

### Supplementary activities to evaluation of sub-activity ADV\_FSP.1

There are no supplementary activities to evaluation of sub-activity ADV\_FSP.1.

### 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 |

### 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 |

### 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 |

## Supplementary activities to TOE design ADV\_TDS

### 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 |

### 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 |

### 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 |

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

## 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 |

## 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 are 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 are configured before the initial usage of the TOE. |

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

## 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 |

## 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 |

## 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).

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

## 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.

## Supplementary activities to independent testing ATE\_IND

### General

There are no supplementary activities supplemented to evaluation of sub-activity ATE\_IND.3.

### 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. |

### 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 |
| 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.

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

## General

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

## Supplementary activities to vulnerability analysis AVA\_VAN

### 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 |
| 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. |

### 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 |
| 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. |

### 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. |

1. (informative)  
     
   Introduction to the basic concepts of ISO/IEC 15408
   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.

* 1. 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 |
| 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.

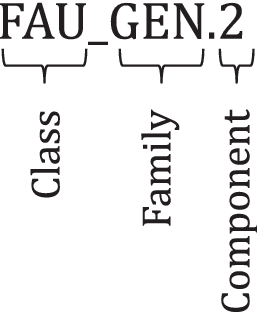


Figure A.1 — Structure of FAU\_GEN.2

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.

* 1. 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.

1. (normative)  
     
   Class FPT: Protection of the TSF
   1. Presentation attack detection (FPT\_PAD)
      1. FPT\_PAD.1 Presentation attack detection
         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.

* + - 1. Operations
         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.

* 1. Biometric capture with presentation attack detection (FPT\_BCP)
     1. FPT\_BCP.1 Check of biometric samples for capture
        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.

* + - 1. 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.

* + 1. 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.

1. (normative)  
     
   Class FIA: Identification and authentication
   1. Enrolment of biometric reference (FIA\_EBR)
      1. FIA\_EBR.1 Check of biometric samples for enrolment
         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.

* + - 1. 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.

* + 1. 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.

* 1. Biometric verification (FIA\_BVR)
     1. FIA\_BVR.1 Biometric verification with high performance
        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.

* + - 1. Operations —Selection

In FIA\_BVR.1.1, the selection of the pair of error rates depends on the PP/ST.

* + 1. FIA\_BVR.2 Timing of user authentication with biometric verification
       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.

* + - 1. Operations — Selection

In FIA\_BVR.2.2, the selection of the pair of error rates depends on the PP/ST.

* + 1. FIA\_BVR.3 User authentication with biometric verification before any action
       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.

* + - 1. Operations — Selection

In FIA\_BVR.3.1, the selection of the pair of error rates depends on the PP/ST.

* + 1. FIA\_BVR.4 Biometric verification not accepting presentation attack instruments
       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.

* + - 1. 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.

* 1. Biometric identification (FIA\_BID)
     1. FIA\_BID.1 Biometric identification with high performance
        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.

* + - 1. Operations —Selection

In FIA\_BID.1.1, the selection of the pair of error rates depends on the PP/ST.

* + 1. FIA\_BID.2 Timing of biometric identification
       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.

* + - 1. Operations — Selection

In FIA\_BID.2.2, the selection of the pair of error rates depends on the PP/ST.

* + 1. FIA\_BID.3 Biometric identification before any action
       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.

* + - 1. Operations — Selection

In FIA\_BID.3.1, the selection of the pair of error rates depends on the PP/ST.

* + 1. FIA\_BID.4 Biometric identification not accepting presentation attack instruments
       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.

* + - 1. 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.

1. (informative)  
     
   Background information on supplementary activities for PAD evaluation
   1. Class APE: Protection Profile evaluation/Class ASE: Security Target evaluation
      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 and with respect to the intended target applications of the TOE.

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.

* + 1. 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.

* 1. Class ADV: Development
     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.

* + 1. 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.

* + 1. 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).

* + 1. 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

* 1. Class AGD: Guidance documents
     1. AGD\_OPE Operational user guidance

For physical interfaces such as capture device, the guidance documentation should describe how users shall present their biometric characteristics to the TOE. Operational user guidance should provide the operator with the instruction to users how to present their biometric characteristics to the TOE and also with responsibility in supervising the capture process for guaranteeing its secure usage. This can be important if the TOE s used in a specific way or if the secure operation of the TOE can be threatened if it is used in a different way. For example, in the case of fingerprint modality, if misplaced presentations can result in an increased false acceptance rate or attack presentation classification error rate, operational user guidance should explain this and provide advice to the operator on monitoring presentations to ensure that misplaced presentations do not occur.

The operational user guidance should describe all configurable parameters which are used by the PAD mechanism and their allowed ranges of value. Typical PAD parameters are for example threshold values which are used to control the PAD decision. The guidance should also state which roles are able to adjust parameters.

The administrator should receive guidance on how to modify these parameters properly and how the modifications change the operation of the TOE. The guidance should clearly identify the range of all parameters that have been considered during the evaluation of the TOE. Additionally, the guidance should give information on how to set theses parameters so that the TOE still operates within the configuration described in the operational user guidance of the TOE.

The administrator and the operator should also be informed about which environmental parameters they are responsible for, and whether the TOE is not working within its evaluated configuration if characteristics of the environment are changed.

If an operator role is considered in the operational environment of the TOE, the operational user guidance should also describe whether an operator is allowed to manually override the decision of the PAD mechanism. If an operator role is allowed to do that, the guidance should specify how the operator role needs to do it. In the case of fingerprint for example, if a genuine biometric characteristic is not recognized as such because of the following situations:

— fingers (or even hands) are missing;

— weakly pronounced fingerprints due to congenital defects;

— injuries like burns.

In such cases, there may be alternative procedures necessary which shall be considered by the operator. Such alternative procedures should then be described by the developer.

It may be necessary to separate the guidance documents for different roles, e.g. administrators, operators, and users. The description of how a user should present his or her biometric characteristic to the capture device is most likely public information. Conversely, details about security relevant parameters should probably not fall into the hands of normal users (as they would then be easily accessible for an attacker as well).

* + 1. AGD\_PRE Preparative procedures

The preparative procedures for PAD mechanisms should provide concrete values for parameters which modify the behaviour of the PAD mechanism and which shall be configured as part of the preparation of the TOE (e.g. thresholds).

If the developer allows the usage of more than one security relevant threshold value, this implies that there is more than one configuration to be tested during testing activity of ATE (see ISO/IEC 19989-3).

For specific TOEs, it may be necessary to calibrate the TOE when it is delivered to the customer. For example, if physical parts of the TOE can become uncalibrated during delivery or installation, then they should be recalibrated.

Considering the hardware part of the TOE, the preparative procedures should describe the environmental conditions that should be met and kept in order to ensure the secure operation of the TOE. Such conditions can be temperature of the environment, air humidity, air pressure, ambient light, electromagnetic radiation, and others.

The TOE may require hardware and/or software components in its operational environment. The preparative procedures should describe how these components should be prepared to be used with the TOE.

* 1. Class ALC: Life-cycle support
     1. ALC\_CMS CM scope

The assurance component ALC\_CMS.4 introduces the requirement that security flaw reports and resolution status should be part of the configuration list. PAIs which are falsely accepted by the PAD mechanism are considered being security flaws. They should be considered in security flaw reports and resolution status accordingly.

Refer to ALC\_FLR in D.4.3 for more information on such security flaws.

* + 1. ALC\_DEL Delivery

The TOE can only be delivered to selected customers in order to prevent unauthorized individuals from gaining information about the TOE. For example, the TOE may not be available in stores, and interested customers can need to contact the developer for a registration. This fact can be used in the assumptions on the operational environment of the TOE since it would be harder to attack a system (specifically to prepare attacks) that is not easily available. However, the developer would need to provide details on how such a controlled distribution is performed so that the evaluator is able to determine its effectiveness with respect to the underlying attack potential.

* + 1. ALC\_FLR Flaw remediation

During the evaluation of the TOE, PAIs which are not detected by the TOE should be recorded as the security flaw.

It is likely that new types of PAI will appear that have not been the subject of testing during the evaluation of the TOE and that those new PAIs can defeat the PAD mechanism of the TOE. Hence, the way in which the developer monitors the evolving threat and incorporates changes in the TOE PAD mechanism to counter the threat is an important consideration for the TOE evaluation.

Therefore, an augmentation of at least ALC\_FLR.1 should be considered being mandatory for any ISO/IEC 15408 evaluation of TOEs contains a PAD mechanism.

The developer should describe how he/she is supposed to be informed about new PAIs that are potent to circumvent the TOE. The developer should particularly describe how such information is received from the customers of the TOE.

The developer should describe how they propose to monitor the evolving threat to the TOE posed by new types of PAI. Monitoring can include:

— information on PAD threats and PAD failures reported by customers of the TOE;

— searches for publicly available articles and reports on tests of PAD capability for biometric systems and technology using the same modality as that used by the TOE;

— obtaining PAD threat and vulnerability reports provided by recognised security incident monitoring organisations such as CSIRT and CERT.

Alternative procedures for TOEs are of particular importance since flaws that cannot be addressed by patches or workarounds are supposed to occur more often for PAD subsystems than for other IT systems. Therefore, the developer shall address alternative procedures.

* + 1. ALC\_TAT Tools and techniques

In ALC\_TAT, the developer should document all tools and techniques which are used to develop, analyse, and implement the TOE in its various hardware and software parts.

For PAD mechanisms, this can include tools and techniques for PAI construction, such as information on materials and construction manuals for different types of PAIs. Documentation on existing PAIs should be provided by the developer.

* 1. Class ATE: Tests
     1. ATE\_FUN Functional tests

The test plan of the developer should provide information like construction manuals that were used for the creation of PAIs, materials that were used, and mixture ratios of materials if applicable. If standard PAI species are provided, the minimum set of PAI types defined should be used, and additional non-standard PAIs types should also be considered during testing.

The developer should document the construction processes for all PAIs and describe relevant aspects like the time of construction. Further, the exact usage of the PAIs during testing should be described.

For all testing activity, it is also necessary that the TOE is in the configuration that is described in the ST. Specifically the PAD parameters that modify the behaviour of the PAD mechanism should therefore be set as required in the ST. If the ST allows multiple settings for security relevant parameters all tests should be conducted for all possible configurations.

Finally, the evaluator should check whether the number of constructed PAIs and the overall test size is documented and meets the minimum needs. See ISO/IEC 19989-3 for more detailed information.

* + 1. ATE\_IND Independent testing

For all testing activity it is essential to ensure that the TOE is operated in the configuration as described in the ST. The PAD parameters that modify the behaviour of the PAD mechanism should therefore be set as required in the ST. If the ST allows multiple settings for security relevant parameters all tests should conducted for all possible configurations.

The evaluator should document the construction processes for all PAIs and describe relevant aspects as the time of construction. Further, the exact usage of the PAIs during testing should be described. For descriptions the evaluator should stick to the level of detail of the descriptions in the standard PAI species if provided.

Finally, the evaluator should report the number of PAIs that were constructed and the number of tests for each PAI.

* 1. Class AVA: Vulnerability assessment
     1. AVA\_VAN Vulnerability analysis

In order to perform penetration testing on the TOE, the evaluator should ensure that the TOE is in the configuration as described in the ST. This includes – but is not limited to – parameters which influence the PAD mechanism and which are identified in the ST.

The vulnerability analysis should consider hints to vulnerabilities that have been found during the evaluation of the ST, development documentation, guidance documents, and public sources. Further information on hints to potential vulnerabilities for PAD are assembled in Annex E.

Construction techniques for the various PAI types that were used for penetration testing should be documented by the evaluator. Relevant information that should be contained therein are at least the used PAI material and the description of the construction process. The evaluator should stick to the level of detail of the descriptions in the standard PAI species if provided.

The evaluator should calculate the attack potential of attacks that exploit specific vulnerabilities of the TOE. For attacks on the PAD mechanism using PAIs, the evaluator should use the approach of calculation of attack potential discussed in Annex F.

1. (informative)  
     
   Other general vulnerabilities
   1. General

This annex gives further guidance on some potential general vulnerabilities that can affect PAD or biometric recognition subsystems. They should be considered by the evaluator during the vulnerabilityanalysis. If the two types of data are collected by separate sensors in the biometric capture device, it can be possible to mount a successful attack by attacking each sensor individually.

* 1. Two-channel attacks

A two-channel attack tries to exploit any separation in space or time that can exist between the capturing process for the biometric characteristic itself and the acquisition of the presentation attack evidence for that characteristic. If the two types of data are collected by separate sensors in the biometric capture device, it can be possible to mount a successful attack by attacking each sensor individually. For example, in a fingerprint biometric system, if the PAI detection collects data from a different part of the biometric capture device than that which captures the biometric sample used for recognition, it can be possible for an attacker to present part of a real finger to the PAI detection area of the biometric capture device and a PAI to the biometric sample capture area. In this case the TOE would be potentially vulnerable to a two-channel attack. This is illustrated in Figure E.1.

|  |  |
| --- | --- |
|  | |
| **a) Regular use** | **b) Two-channel attack** |

Figure E.1 — Two-channel attack

This attack can also exploit timing aspects of the acquisition processes when presentation attack detection and capturing are performed in sequence. The evaluators should be alert to the possibility of subversion of PAD techniques by two-channel attacks.

During the evaluation of the development documentation, the evaluator should gain confidence that two-channel attacks are not possible. The information gathered during the evaluation of the ADV and AGD aspects may be a good starting point for this investigation.

If an examination of the TOE design indicates that there is a possibility that a two-channel attack can succeed, evaluators should conduct penetration testing to ascertain whether the vulnerability exists in practice.

* 1. Feedback provided by TOEs

Feedback provided by a TOE on the results of presentation attempts can be helpful to the evaluator who is conducting security evaluations. Such information can include: capture result (success/failure and reason), capture sample quality information, score from the PAD subsystem, PAD decision, etc.

However, it is important to prevent feedback information from falling into the hands of regular users who can be attackers. Attackers can use feedback information to assist an attack and increase the likelihood of it being successful. The protection of feedback information is an information security matter that forms part of the security evaluation of the TOE.

The evaluator should consider whether such information can be used by an attacker to assist presentation attacks. For example, if it is possible to identify PAI properties that result in a lower (or higher) score value, it would be possible to improve PAIs more efficiently using a hill-climbing approach.

The information derived from the evaluation of ADV\_FSP can be valuable for this investigation.

If an examination of the functional specification of the TOE does not confirm that no security compromising feedback is produced, the evaluator should conduct a penetration test to determine whether feedback exists that can be exploited by an attacker.

1. (normative)  
     
   Attack potential and TOE resistance
   1. Calculating attack potential
      1. General

Attack potential is a function of expertise, resources and motivation, as is written in ISO/IEC 18045. Regarding motivation, see ISO/IEC 18045:2008, B.4.1.1.

This clause F.1 describes the general approach for calculating attack potential. Adapted versions (specific to some use cases or simplified for low level of resistance), together with some examples of attacks are introduced in annexes G to H.

* + 1. Identification and exploitation of attacks
       1. Identification of attacks

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

* + - 1. Exploitation of attacks

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

NOTE 1 For the evaluator, the work of the identification phase needs to be fully performed: developing hardware and software, creating PAIs if any, etc. The attack potential of this phase corresponds to the "real spending" in defining the attack. For the exploitation, it is not necessary to perform the work again and the attack potential can correspond to an evaluation of the necessary effort for each factor.

NOTE 2 Exploitation consisting in applying scripts, it is expected that some factor values are reduced from the identification phase, in particular "elapsed time" and "expertise". For the same reason, the "knowledge of the TOE" factor is not applicable in the exploitation phase (all the knowledge is scripted).

* + 1. Factors to be considered

As in ISO/IEC 18045, the factors to be considered consist of ***elapsed time, expertise, knowledge of the TOE, window of opportunity, and equipment***. but ***window of opportunity*** is divided into two subfactors ***window of opportunity (access to the TOE)*** and ***window of opportunity (access to biometric characteristics)***.

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

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

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

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

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

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

NOTE The term "layperson" is used for gender neutrality.

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

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

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

NOTE 1 As previously noted, exploitation expertise is usually lower than identification expertise. Layperson or Proficient can be considered as typical value for expertise in the exploitation phase. For the same reason, the multiple expert level is excluded from the exploitation phase.

NOTE 2 As all the factors, higher attack potential would require specific justifications from the evaluator.

***Knowledge of the TOE*** refers to the amount of knowledge of system required to perform the attack.

For instance, format of the acquired samples, size and resolution of acquisition systems, specific format of templates, but also specifications and implementation of countermeasures are knowledge that can be required to set up an attack.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

***Window of opportunity (access to biometric characteristics)***

Security evaluations of ISO/IEC 15408 are dedicated to evaluating the intrinsic resistance of a system. Due to the potential number of attack paths (with or without the cooperation of an enrolled subject for example) the evaluation does not take into account the way a real biometric characteristic is acquired. For presentation attack detection, the vulnerability analysis is based on the hypothesis that a real "image" is available, and the attack potential only concerns the creation and the presentation of a PAI.

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

a) Not needed or Immediate. Not needed if the attacker does not need to access any biometric characteristics. Immediate is for 2D face, signature image, and voice. Samples of these modalities can be collected without difficulty, even without direct contact with an enrolled data subject (an exploration of the web and the social networks and so forth).

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

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

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

NOTE 1 The above distribution of modalities per level is subject to modification depending on the evolution of technologies and usage. The current distribution is to be seen as guidance for the evaluator, who shall adapt the attack potential to state-of-the-art.

NOTE 2 Rating the resistance of a system is based on attack potential the successful attacks and verifying that no successful attack is found at the targeted level. Some attacks do not need real biometric data to be available, for example, attacks based on synthetic images or templates generation. In such a case, this factor needs to be considered to be immediate.

NOTE 3 For most of the TOEs, this criteria has no impact during identification but some systems are not necesseraly fully usable by the evaluator (e.g. if enrolment is not part of the TOE) and thus the evaluator can coinsider the cotation in identification phase as well.

Editor’s note: An alternative definition could be the following one – to be discussed

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

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

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

The levels are as follows:

1. *Without notice* is for making an artefact with samples that can be collected without any contact with an enroled subject. For example, 2D face images uploaded on the Internet and latent fingerprint images on a glass can be collected without notice of the subject.
2. *Non-cooperative* is for making an artefact with samples that need to be collected directly from an enroled subject in a short period of time without full cooperation from the subject. For example, iris or vein images need to be acquired with a high resolution or infrared camera, however, such images can be taken in a moment without full control of the subject.
3. *Cooperative* is for making an artefact with samples that need to be collected directly from an enroled subject with full cooperation from the subject. For example, the acquisition of a detailed 3D face scan of the subject takes time and requires full cooperation from the subject.

**Note** Rating the resistance of a system is based on rating the successful attacks and verifying that no successful attack is found at the targeted level. Some attacks do not need real biometric data to be available, for example, attacks based on synthetic images or template generation. In such a case, this factor has to be considered to be *Without notice*.

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

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

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

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

* + 1. Calculation of attack potential

Table F.1 identifies the factors discussed in F.1.3 and associates numeric values with the total value of each factor.

Table F.1 — Calculation of attack potential

|  |  |  |
| --- | --- | --- |
| **Factor** | **Value** | |
| **Identification** | **Exploitation** |
| **Elapsed time** |  |  |
| ≤ one day | 0 | 0 |
| ≤ one week | 1 | 2 |
| ≤ two weeks | 2 | 4 |
| ≤ one month | 4 | 8 |
| > one month | 8 | 16 |
| **Expertise** |  |  |
| Layperson | 0 | 0 |
| Proficient | 2 | 4 |
| Expert | 4 | 8 |
| Multiple experts | 8 | Not applicable |
| **Knowledge of TOE** |  |  |
| Public | 0 | Not applicable |
| Restricted | 2 | Not applicable |
| Sensitive | 4 | Not applicable |
| Critical | 8 | Not applicable |
| **Window of opportunity**  **(Access to TOE)** |  |  |
| Easy | 0 | 0 |
| Moderate | 2 | 4 |
| Difficult | 4 | 8 |
| **Window of opportunity**  **(Access to biometric  characteristics)** |  |  |
| Immediate | Not applicable (or 0) | 0 |
| Easy | Not applicable (or 2 if the evaluator has restrictions during identification) | 2 |
| Moderate | Not applicable (or 4 if the evaluator has restrictions during identification) | 4 |
| Difficult | Not applicable (or 8 if the evaluator has restrictions during identification) | 8 |
| **Equipment** |  |  |
| Standard | 0 | 0 |
| Specialized | 2 | 4 |
| Bespoke | 4 | 8 |

In order to calculate the attack potential value of the entire attack, the evaluator shall add all the values of all the factors in identification phase and exploitation phase. Table F.1 is intended as a guide. Evaluator may modify the table with a proper justification.

Note: when assessing the attack potential, an attack is considered as not practical if at least one criteria is considered as not practical.

* + 1. Rating of vulnerabilities and TOE resistance

The "Values" column of Table F.2 indicates the range of attack potential values (calculated using Table A.1) of an attack scenario that results in the SFRs being undermined.

Table F.2 — Rating of vulnerabilities and TOE resistance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Values** | **Attack potential required to expoit scenario:** | **TOE resistant to attackers with attack potential of:** | **Meets assurance components:** | **Failure of components:** |
| <10 | Basic | No rating | - | AVA\_VAN.1,  AVA\_VAN.2,  AVA\_VAN.3,  AVA\_VAN.4,  AVA\_VAN.5 |
| 10–19 | Enhanced– Basic | Basic | AVA\_VAN.1,  AVA\_VAN.2 | AVA\_VAN.3,  AVA\_VAN.4,  AVA\_VAN.5 |
| 20–29 | Moderate | Enhanced– Basic | AVA\_VAN.1,  AVA\_VAN.2,  AVA\_VAN.3 | AVA\_VAN.4,  AVA\_VAN.5 |
| 30–39 | High | Moderate | AVA\_VAN.1,  AVA\_VAN.2,  AVA\_VAN.3,  AVA\_VAN.4 | AVA\_VAN.5 |
| ≥40 | Beyond– High | High | AVA\_VAN.1,  AVA\_VAN.2,  AVA\_VAN.3,  AVA\_VAN.4,  AVA\_VAN.5 | - |

1. (normative)  
     
   Adapted Versions of Attack potential

Editor’s note: contributions from experts are invited. Some contributions are already added here but need to be reviewed/discussed.

* 1. Calculating attack potential for specific use cases
     1. Mobile fingerprint verification

Three levels of assurance, Basic, Substantial and High, are defined for the mobile fingerprint PA to simplify the attack potential calculation. All evaluations should choose either of levels. Evaluators don’t need to estimate the value for attack potential factor because those values are prefixed for each level to simplify the attack potential calculation.

* + - 1. Choosing the level

Three levels of assurance are defined based on the criticality of asset protected by the mobile fingerprint verification. Some use cases may not exactly fit to the one described in the following table, but the developer should choose one of them that is the closest to its use case or considering prefixed attack potential factors defined in the following section.

AVA\_VAN assurance component is also prefixed for each level. The developer can’t select the other components such as AVA\_VAN.2 or AVA\_VAN.4 if the evaluations conform to this Annex.

|  |  |
| --- | --- |
| Level | Asset and corresponding use case |
| Basic  (AVA\_VAN.1) | Fingerprint verification is used for unlocking a mobile device that is not used for the sensitive or critical services.  Attackers can gain a target user’s private information if the PA can succeed. |
| Substantial  (AVA\_VAN.3) | Fingerprint verification is used for the sensitive services such as remote identify proofing to create a banking account and sufficient for commercial requirements.  Attackers can gain financial profit if the PA can succeed. |
| High  (AVA\_VAN.5) | Fingerprint verification is used to access the national security information and useful for government requirements.  Attackers can access the national security information if the PA can succeed. |

* + - 1. Key factors for classification

Vital information to create the high-quality fingerprint PAI is a) available information about target fingerprint (i.e., Window of opportunity (Access to biometric characteristics)), and b) available information about the PAD (i.e., Knowledge of the TOE).

Mobile fingerprint PAs are classified into three based on these two factors. Knowledge of the TOE has four level (Public, Restricted, Sensitive and Critical) but the PAD attack potential doesn’t use Sensitive to simplify the calculation.

|  |  |
| --- | --- |
| Level | Attack |
| Basic  (AVA\_VAN.1) | Attacker can gain only latent fingerprint of a target user.  All information required for AVA\_VAN.1 shall be provided to the evaluator. In principle, detail PAD information isn’t available (The ST simply claims that the TOE can reject the PA).  Corresponding attack potential factors are estimated as follows.  “Window of opportunity (Access to biometric characteristics)”: without notice (E)  “Knowledge of the TOE”: Public (I) |
| Substantial  (AVA\_VAN.3) | The attacker can gain target user’s fingerprint information indirectly from an enrolled template, latent fingerprint, high-resolution photo of finger or fingertip friction sound etc to create the PAIs. The attacker should also create synthetic fingerprints without such indirect information that can fortuitously match with a large number of other fingerprints (e.g., MasterPrint) and measure the success rate.  All information required for AVA\_VAN.3 shall be provided to the evaluator. In principle, high level design information of PAD (The ST explains that, for example, the TOE detects the presence of sweat pores as a PAD measure. Architectural design describes how the senser and firmware interact to detect the sweat pores and determine whether the PAI is presented or not) should be provided to the evaluator.  Corresponding attack potential factors are estimated as follows.  “Window of opportunity (Access to biometric characteristics)”: Non-cooperative (E)  “Knowledge of the TOE”: Restricted (I) |
| High  (AVA\_VAN.5) | Attacker can gain any fingerprint information from a fully cooperative target user.  All information required for AVA\_VAN.5 shall be provided to the evaluator. In principle, TOE’s source code that implements the PAD should be provided to the evaluator. If the TOE implements a deep learning model trained using training data, training data and architecture of deep learning model should also be provided.  Evaluator doesn’t need to test the Basic and Substantial level PAIs that are created from fingerprint information gained indirectly from the target. There is no possibility for the Basic and Substantial level PAIs to succeed the PA if the PAI created from detail original fingerprint image can’t bypass the PAD.  Corresponding attack potential factors are estimated as follows.  “Window of opportunity (Access to biometric characteristics)”: Cooperative (E)  “Knowledge of the TOE”: Critical (I) |

I: Identification, E: Exploitation

* + - 1. Prefixed attack potential table for each level

Presentation attack scenario is that the attacker simply creates the PAI based on the target user’s fingerprint information and the PAD information if available and present it to the mobile device. The mobile device is securely configured and managed as described in the Mobile Device Protection Profile (MDPP \*1).

\*1) https://www.niap-ccevs.org/profile/Info.cfm?PPID=468&id=468

Some factors like Elapsed Time (E) can be determined because the MDPP assumes that mobile user will immediately notify the administrator if the device is lost or stolen, so Elapsed Time (E) should be “⇐ one day”.

The other factors like Elapsed Time (I) should proportionally increase according to the level. They are prefixed referring examples of attack potential calculation in the other technology area like smart cards.

|  |  |  |  |
| --- | --- | --- | --- |
| Factor | Basic | Substantial | High |
| Elapsed Time (I) | ⇐ one week | ⇐ two weeks | ⇐ three months |
| Elapsed Time (E) | ⇐ one day | | |
| Expertise (I) | Layman | Expert | Multiple experts |
| Expertise (E) | Layman | | |
| Knowledge of TOE (I) | Public | Restricted | Critical |
| Window of Opportunity (Access to TOE) (I) | Easy | | |
| Window of Opportunity (Access to TOE) (E) | Moderate | | |
| Window of Opportunity (Access to Biometric Characteristics) (E) | without notice | Non-cooperative | Cooperative |
| Equipment (I) | Standard | Specialised | Bespoke |
| Equipment (E) | Standard | | |
| Total value | 3 | 14 | 34 |

I: Identification, E: Exploitation

* + 1. Online scenarios
       1. Use of the TOE

In addition to the windows of opportunity – Access to TOE – criteria, the evaluator can consider the difficulty to use the TOE in an operationally representative setting. The corresponding values should be added to the Access to TOE values.

This applies in particular to system when remote operators or additional components are interacting with the TOEs, but not accessible to the evaluator. A typical example is remote ID proofing with skilled operators. In such cases, the concept of degree of scrutiny of the TOE is enclosed within the criteria “online use of the TOE”.

- None: the attacker is not supervised or is not constrained on the use of the TOE while executing an attack.

- Overseen: there is at least a security agent or an operator trained for fraud detection or external components that are interacting with the TOE, who oversees the usage of the TOE. However, the control is done quickly in order to be efficient in time and is done remotely.

- Not practical: There is no way to attempt an attack without being checked or fully blocked if the attack is unsuccessful. The evalutor can decide that an attack is “not practical” when the level of security control is high enough to consider that an attacker is not enough confident to perform an attack.

|  |  |  |
| --- | --- | --- |
| **Window of opportunity**  **(Use of the TOE)** |  |  |
| None | 0 | 0 |
| Overseen | 2 | 3 |
| Not practical | x | X |

Editor’s note: to be completed – cf. concept of degree of scrutiny in CEN TC224 WG18 TS on digital injection attacks

* + - 1. Replicability

For online and quasi-automated scenarios, an additional criteria shall be assessed by the evaluator: replicability.

This adds no value to the identification phase but will downgrade the total value in exploitation phase with the principle that if an attack is high and can be scaled to attack many instances in parallel, then the overall attack potential cotation should be considered as moderate instead of high. It reflects the benefit optimization of the attack when averaged over many instances (either several systems or targeting several users in parallel).

|  |  |  |
| --- | --- | --- |
| **Replicability** |  |  |
| Easy | NA | -6 |
| Moderate | NA | -3 |
| Difficult | NA | 0 |

Editor’s note: to be completed – cf. also [https://fidoalliance.org/specs/fido-security-requirements/FIDO-L1+-Application-of-Attack-Potential-v1.0-fd-20211102.html#calculation-of-attack-potential](https://fidoalliance.org/specs/fido-security-requirements/FIDO-L1+-Application-of-Attack-Potential-v1.0-fd-20211102.html" \l "calculation-of-attack-potential)

* + 1. Digital attacks
       1. Elapsed time

A more granular scale can be considered by the evaluator for digital attacks to better capture the competitive landscape where attackers would try to focus on easy to attack systems first.

|  |  |  |
| --- | --- | --- |
| **Elapsed time** | Identification | Exploitation |
| **< one hour** | 0 | 0 |
| ≤ one day | 1 | 3 |
| < three days | 2 | 4 |
| ≤ one week | 3 | 6 |
| ≤ two weeks | 4 | 7 |
| ≤ one month | 6 | 8 |
| > one month | 8 | 16 |
| Not Practical | x | x |

* + - 1. Expertise

Given the proliferation of digital toolkits for digital exploits, an additional category may be considered that is about someone being digitally skilled – without being considered as proficient in the biometric technologies – to be able to find, adapt and use existing scripts and tools.

|  |  |  |
| --- | --- | --- |
| **Expertise** |  |  |
| Layperson | 0 | 0 |
| Digitally skilled | 1 | 2 |
| Proficient | 2 | 4 |
| Expert | 4 | 8 |
| Multiple experts | 8 | Not applicable |

* 1. Calculating attack potential for TOEs with low level of resistance
  2. Mapping of levels of assurance with EU framework (added here as per request from some experts but feasibility of this discussion has to be confirmed/discussed)

1. (informative)  
     
   Examples of attack potential

Editor’s note: general example to be included in part 1 are invited. Consider cases of injection attacks, deepfakes, masterprints, …

* 1. Example 1
  2. Example 2

Bibliography

[1] ISO/IEC 19792:2009, Information technology — Security techniques — Security evaluation of biometrics

[2] ISO/IEC 19795-1, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

[3] ISO/IEC 29794‑1:2016, Information technology — Biometric sample quality — Part 1: Framework

[4] ISO/IEC 30107‑1:2016, Information technology — Biometric presentation attack detection — Part 1: Framework

[5] ISO/IEC 30107‑3:2017, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

[6] Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies FSDPP\_OSP v1.7, November 2009

[7] Ellingsgaard J., Sousedik C., Busch C. Detecting Fingerprint Alterations by Orientation Field and Minutiae Orientation Analysis, in Proceedings of the 2nd International Workshop on Biometrics and Forensics 2014 (IWBF 2014), 27-28th March 2014, Valletta, Malta, (2014)

[8] M. Gomez-Barrero, J. Galbally, A. Morales, M. Ferrer, J. Fierrez, and J. Ortega-Garcia. A novel hand reconstruction approach and its application to vulnerability assessment. *Information Sciences*, 268:103–121, 2014

[9] Gottschlich C., Mikaelyan A., Olsen M., Bigun J., Busch C. Improving Fingerprint Alteration Detection, in Proceedings 9th International Symposium on Image and Signal Processing and Analysis (ISPA 2015), 7-9 September, Zagreb, Croatia, (2015)

[10] Haraksim R., Anthonioz A., Champod C., Olsen M., Ellingsgaard J., Busch C. Altered fingerprint detection - Algorithm performance evaluation, in Proceedings of the 4th International Workshop on Biometrics and Forensics 2016 (IWBF 2016), 3-4th March 2016, Limassol, Cyprus, (2016)

[11] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters*, 32(12):1643–1651, 2011

[12] S. Yoon, J. Feng, and A. K. Jain, Altered Fingerprints: Analysis and Detection, *IEEE Trans. Pattern Anal. Mach. Intell*., vol. 34, no. 3, pp. 451–464, (2012)