INTERNATIONAL STANDARD

ISO/IEC 19989-1

First edition
2020-09

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

Part 1: **Framework**

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

Partie 1: Cadre

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

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **vi**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **3**
5 General remarks ... **4**
6 Vulnerabilities in biometric systems and security evaluation ... **5**
6.1 Categorization of common vulnerabilities of biometric systems ... 5
6.2 Biometric system and presentation attack detection ... 8
6.3 Categorization of TOEs in relation to the type of evaluation ... 9
6.3.1 Biometric recognition performance evaluation ... 9
6.3.2 PAD evaluation ... 10
7 Extended security functional components to Class FPT: Protection of the TSF ... **10**
7.1 General ... 10
7.2 Presentation attack detection (FPT_PAD) ... 11
7.2.1 Family behaviour ... 11
7.2.2 Component levelling ... 11
7.2.3 Management of FPT_PAD.1 ... 11
7.2.4 Audit of FPT_PAD.1 ... 11
7.2.5 FPT_PAD.1 Presentation attack detection ... 11
7.3 Biometric capture with presentation attack detection (FPT_BCP) ... 12
7.3.1 Family behaviour ... 12
7.3.2 Component levelling ... 12
7.3.3 Management of FPT_BCP.1 ... 12
7.3.4 Management of FPT_BCP.2 ... 13
7.3.5 Audit of FPT_BCP.1 ... 13
7.3.6 Audit of FPT_BCP.2 ... 13
7.3.7 FPT_BCP.1 Check of biometric samples for capture ... 13
7.3.8 FPT_BCP.2 Biometric capture with low failure rate ... 13
8 Extended security functional components to Class FIA: Identification and authentication ... **14**
8.1 General ... 14
8.2 Enrolment of biometric reference (FIA_EBR) ... 14
8.2.1 Family behaviour ... 14
8.2.2 Component levelling ... 14
8.2.3 Management of FIA_EBR.1 ... 15
8.2.4 Management of FIA_EBR.2 ... 15
8.2.5 Audit of FIA_EBR.1 ... 15
8.2.6 Audit of FIA_EBR.2 ... 15
8.2.7 FIA_EBR.1 Check of biometric samples for enrolment ... 15
8.2.8 FIA_EBR.2 Biometric enrolment with low failure to enrol rate ... 16
8.3 Biometric verification (FIA_BVR) ... 16
8.3.1 Family behaviour ... 16
8.3.2 Component levelling ... 16
8.3.3 Management of FIA_BVR.1 ... 16
8.3.4 Management of FIA_BVR.2 ... 16
8.3.5 Management of FIA_BVR.3 ... 17
8.3.6 Management of FIA_BVR.4 ... 17
8.3.7 Audit of FIA_BVR.1 ... 17
8.3.8 Audit of FIA_BVR.2 ... 17

© ISO/IEC 2020 – All rights reserved

8.3.9 Audit of FIA_BVR.3 17
8.3.10 Audit of FIA_BVR.4 17
8.3.11 FIA_BVR.1 Biometric verification with high performance 18
8.3.12 FIA_BVR.2 Timing of user authentication with biometric verification 18
8.3.13 FIA_BVR.3 User authentication with biometric verification before any action 18
8.3.14 FIA_BVR.4 Biometric verification not accepting presentation attack instruments 19
8.4 Biometric identification (FIA_BID) 19
8.4.1 Family behaviour 19
8.4.2 Component levelling 19
8.4.3 Management of FIA_BID.1 20
8.4.4 Management of FIA_BID.2 20
8.4.5 Management of FIA_BID.3 20
8.4.6 Management of FIA_BID.4 20
8.4.7 Audit of FIA_BID.1 20
8.4.8 Audit of FIA_BID.2 20
8.4.9 Audit of FIA_BID.3 21
8.4.10 Audit of FIA_BID.4 21
8.4.11 FIA_BID.1 Biometric identification with high performance 21
8.4.12 FIA_BID.2 Timing of biometric identification 21
8.4.13 FIA_BID.3 Biometric identification before any action 22
8.4.14 FIA_BID.4 Biometric identification not accepting presentation attack instruments 22

9 Supplementary activities to ISO/IEC 18045 on Class APE: Protection Profile evaluation 22

10 Supplementary activities to ISO/IEC 18045 on Class ASE: Security Target evaluation 23

11 Supplementary activities to ISO/IEC 18045 on Class ADV: Development 24
11.1 Supplementary activities to security architecture ADV_ARC 24
11.2 Supplementary activities to functional specification ADV_FSP 24
11.2.1 Supplementary activities to evaluation of sub-activity ADV_FSP.1 24
11.2.2 Supplementary activities to evaluation of sub-activity ADV_FSP.2 24
11.2.3 Supplementary activities to Evaluation of sub-activity ADV_FSP.3 25
11.2.4 Supplementary activities to Evaluation of sub-activity ADV_FSP.4 26
11.3 Supplementary activities to TOE design ADV_TDS 27
11.3.1 Supplementary activities to evaluation of sub-activity ADV_TDS.1 27
11.3.2 Supplementary activities to evaluation of sub-activity ADV_TDS.2 28
11.3.3 Supplementary activities to evaluation of sub-activity ADV_TDS.3 28

12 Supplementary activities to ISO/IEC 18045 on Class AGD: Guidance documents 29
12.1 Supplementary activities to operational user guidance AGD_OPE 29
12.2 Supplementary activities to preparative procedures AGD_PRE 30

13 Supplementary activities to ISO/IEC 18045 on Class ALC: Life-cycle support 30
13.1 Supplementary activities to CM support ALC_CMS 30
13.2 Supplementary activities to Delivery ALC_DEL 31
13.3 Supplementary activities to flaw remediation ALC_FLR 31

14 Supplementary activities to ISO/IEC 18045 on Class ATE: Tests 31
14.1 Supplementary activities to functional tests ATE_FUN 31
14.2 Supplementary activities to independent testing ATE_IND 32
14.2.1 General 32
14.2.2 Supplementary activities to evaluation of sub-activity ATE_IND.1 32
14.2.3 Supplementary activities to Evaluation of sub-activity ATE_IND.2 33

15 Supplementary activities to ISO/IEC 18045 on Class AVA: Vulnerability assessment 35
15.1 General 35
15.2 Supplementary activities to vulnerability analysis AVA_VAN 35
15.2.1 Supplementary activities to evaluation of sub-activity AVA_VAN.2 35
15.2.2 Supplementary activities to evaluation of sub-activity AVA_VAN.3 36
15.2.3 Supplementary activities to evaluation of sub-activity AVA_VAN.4 37

 © ISO/IEC 2020 – All rights reserved

Annex A (informative) **Introduction to the basic concepts of ISO/IEC 15408** **39**
Annex B (normative) **Class FPT: Protection of the TSF** **41**
Annex C (normative) **Class FIA: Identification and authentication** **43**
Annex D (informative) **Background information on supplementary activities for PAD evaluation** **47**
Annex E (informative) **Other general vulnerabilities** **54**
Annex F (normative) **Attack potential and TOE resistance** **56**
Bibliography **62**

© ISO/IEC 2020 – All rights reserved

Foreword

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

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

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

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

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

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

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

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

© ISO/IEC 2020 – All rights reserved

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.

© ISO/IEC 2020 – All rights reserved

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

Part 1: Framework

1 Scope

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

— extended security functional components to SFR Classes in ISO/IEC 15408-2;

— supplementary activities to methodology specified in ISO/IEC 18045 for SAR Classes of ISO/IEC 15408-3.

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

2 Normative references

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

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

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

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

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

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

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

3 Terms and definitions

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

© ISO/IEC 2020 – All rights reserved

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]

© ISO/IEC 2020 – All rights reserved

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

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

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

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

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

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

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

3.8
presentation attack detection
PAD
automated determination of a presentation attack

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

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

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

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

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

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

4 Symbols and abbreviated terms

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

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

© ISO/IEC 2020 – All rights reserved