



DPC: 24/30468619 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 05 July 2024

Origin: International

Latest date for receipt of comments: 28 August 2024

Project No. 2023/00149

Responsible committee: IST/33/3 Security Evaluation, Testing and Specification

Interested committees:

Title: Draft BS EN ISO/IEC 19792 BS EN ISO/IEC 19792 Information security, cybersecurity and privacy protection -General principles of security evaluation of biometric systems.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 28 August 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 19792

Information security, cybersecurity and privacy protection — General principles of security evaluation of biometric systems

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-07-05

Voting terminates on:
2024-09-27

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 19792:2024(en)

Full document details: 24/30468619 DC

© ISO/IEC 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 General	1
3.2 Biometric systems	3
3.3 Biometric processes	5
3.4 Recognition performance	6
3.5 Presentation attack detection	7
4 Symbols (and abbreviated terms)	7
5 Overview of security evaluation of biometric systems	8
5.1 Biometric systems and their vulnerabilities	8
5.2 Approach of security evaluation of biometric systems	9
6 Threat and vulnerability analysis	10
6.1 Overview	10
6.2 Threats and vulnerabilities for considerations	11
6.2.1 Overview	11
6.2.2 Performance limitations	12
6.2.3 Hostile environment	12
6.2.4 Insufficient controls of the enrolment process	13
6.2.5 Difficulty of concealing biometric characteristics	13
6.2.6 Leakage and alteration of biometric data	13
6.2.7 Synthesised wolf biometric samples	14
6.2.8 PAI of biometric characteristics	14
6.2.9 Similarity due to blood relationship	14
6.2.10 Special biometric characteristics	15
6.2.11 Modification of biometric characteristics	15
6.2.12 Miscellaneous threat and vulnerabilities	15
7 Evaluation of biometric recognition performance and related vulnerabilities	15
7.1 Overview	15
7.2 Concept – Testing security-relevant error rates	16
7.3 Independent testing	16
7.4 Consideration of impact of error rates	17
8 Evaluation of biometric specific vulnerabilities	17
8.1 Overview	17
8.2 Vulnerability assessment for presentation attacks and other potential threats	18
8.2.1 Application note	18
8.2.2 Performance limitations	18
8.2.3 Hostile environment	19
8.2.4 Procedural vulnerabilities around the enrolment process	19
8.2.5 Difficulty of concealing biometric characteristics	19
8.2.6 Leakage and alteration of biometric data	20
8.2.7 Synthesised wolf biometric samples	20
8.2.8 PAI of biometric characteristics	21
8.2.9 Similarity due to blood relationship	22
8.2.10 Special biometric characteristics	22
8.2.11 Modification of biometric characteristics	22
9 Privacy	23
9.1 Overview	23
9.2 Data protection	24

9.3	Account deactivation of biometric reference data.....	24
9.4	De-enrolment.....	24
Bibliography		25

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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

For an explanation on 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 the following URL www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27

This second edition replaces the first edition published in 2009, the structure of which has been technically revised in harmonization with other security evaluation documents. Accordingly, the title is replaced from "Security evaluation of biometrics" considering the relation with ISO/IEC 19989 series that are based on ISO/IEC 15408 series and ISO/IEC 18045.

Introduction

This document does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in this document are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme.

This document defines various areas that are important to be considered during a security evaluation of a biometric system. These areas are represented by the following clauses:

[Clause 5](#) explains the outline of security evaluation of biometric systems,

[Clause 6](#) overviews the threats and vulnerabilities to biometric systems that should be considered for the evaluation,

[Clause 7](#) describes the evaluation of biometric specific vulnerabilities related to recognition performance,

[Clause 8](#) deals with the evaluation of biometric specific vulnerabilities related to presentation attack detection, and

[Clause 9](#) overviews the evaluation of privacy.

This document is relevant to both evaluator and developer communities. It provides guidance on performing a security evaluation of a biometric system. It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations.

Although this document is independent of any specific evaluation scheme, it serves as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

This document refers to and utilizes other biometric standards, notably those for biometric performance testing and reporting and evaluation of presentation attack detection from ISO/JTC1 SC 37. These standards have been adapted as necessary for the specific requirements of biometric security evaluation.

Any organizations who want to purchase or use secure biometric systems can also refer this document to set proposer security requirements for biometric systems or devices.

ISO/IEC 19989 series, named Criteria and methodology for security evaluation of biometric systems, for security evaluation of biometric products based on ISO/IEC 15048 series have already been published. As in the title, ISO/IEC 19989 series are based on ISO/IEC 15408 series. This document can be seen as an introductory document to them. In addition, this document is also a general guidance to design and execute security evaluation methodologies of biometric systems that do not aimed for ISO/IEC 15408 conformance.

Information security, cybersecurity and privacy protection — General principles of security evaluation of biometric systems

1 Scope

This document specifies the subjects to be addressed during a security evaluation of a biometric system.

This document provides an overview of the main biometric-specific aspects, i.e., recognition performance, presentation attack detection, and privacy, and specifies principles to be considered for the security evaluation of a biometric system.

This document does not address the non-biometric aspects which can form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

This document does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in this document are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme.

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 19795-1:2021, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 24745:2022, *Information security, cybersecurity and privacy protection — Biometric information protection*

ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

ISO/IEC 30136:2018, *Information technology — Performance testing of biometric template protection schemes*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1 General

3.1.1

assurance

grounds for confidence that a target of evaluation meets the security functional requirements

[SOURCE: FDIS ISO/IEC 15408-1, 3.6]

3.1.2

attacker

person seeking to exploit potential vulnerabilities of a biometric system

3.1.3

authentication

provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.1.4

biometric

of or having to do with biometrics

Note 1 to entry: The use of biometric as a noun, to mean for example, biometric characteristic (37.01.02), is deprecated.

EXAMPLE 1 Incorrect usage #1: ICAO resolved that face is the biometric most suited to the practicalities of travel documents.

EXAMPLE 2 Correct usage #1: ICAO resolved that face recognition is the biometric mode (37.02.05) most suited to the practicalities of travel documents.

EXAMPLE 3 Incorrect usage #2: The biometric recorded in my passport is a facial image.

EXAMPLE 4 Correct usage #2: The biometric characteristic recorded in my passport is a facial image.

Note 2 to entry: Since the late 19th century the terms biometrics and biometry have been used with the general meaning of counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences.

[SOURCE: ISO/IEC 2382-37:2022, 37.01.01]

3.1.5

biometric recognition

biometrics

automated recognition of individuals based on their biological and behavioural characteristics

Note 1 to entry: In the field of biometrics (as defined in this document), "Individual" is restricted in scope to refer only to humans.

Note 2 to entry: The general meaning of biometrics encompasses counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences.

Note 3 to entry: Biometric recognition encompasses biometric verification (37.08.03) and biometric identification.

Note 4 to entry: Automated recognition implies that a machine-based system is used for the recognition either for the full process or assisted by a human being.

Note 5 to entry: Behavioural and biological characteristics cannot be completely separated which is why the definition uses 'and' instead of 'and/or'. For example, a fingerprint image results from the biological characteristics of the finger ridge patterns and the behavioural act of presenting the finger.

Note 6 to entry: Use of 'authentication' as a synonym for "biometric verification or biometric identification" is deprecated; the term biometric recognition is preferred.

[SOURCE: ISO/IEC 2382-37:2022, 37.01.03]

3.1.6

developer

organization responsible for the development of the target of evaluation

[SOURCE: ISO/IEC 15408-1:2022, 3.33]

Note 1 to entry: Target of evaluation is defined as follows in ISO/IEC 15408-1:2022: