



DPC: 24/30463746 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: 04 July 2024

Origin: International

Latest date for receipt of comments: 27 August 2024

Project No. 2022/02251

Responsible committee: IST/33/5 Identity Management and Privacy Technologies

Interested committees:

Title: Draft BS EN ISO/IEC 27553-2 BS EN ISO/IEC 27553-2 Information security, cybersecurity and privacy protection - Security and privacy requirements for authentication using biometrics on mobile devices. Part 2: Remote modes.

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 27 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 27553-2

Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices —

Part 2: Remote modes

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-07-04

Voting terminates on:
2024-09-26

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 27553-2:2024(en)

Full document details: 24/30463746 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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	5
5 Security and privacy considerations	6
5.1 General	6
5.2 Security challenges common to all biometric systems	6
5.3 Why one would choose to go for remote modes instead of local modes?	7
5.4 Security and privacy challenges specific to remote modes	8
5.4.1 General	8
5.4.2 Sharing biometric information with remote services	8
5.4.3 Security heterogeneity of remote services information system	8
6 System description	8
6.1 Generic architecture	8
6.2 Entities and components	9
6.2.1 Biometric system	9
6.2.2 Relying Party agent	10
6.2.3 Authentication agent	10
6.2.4 Relying Party server	10
6.2.5 Authentication server	10
6.3 Biometric system application models	10
6.4 Types of authentication workflow for remote mode	12
7 Information assets	12
8 Threat analysis	14
8.1 Threats related to the biometric system	14
8.2 Threats related to the authentication and relying party agents	15
8.3 Threats related to the authentication and relying party servers	17
8.4 Threats to communication between agents and servers	17
9 Security requirements and recommendations	18
9.1 General	18
9.2 Biometric system	18
9.3 Mobile Device - side	19
9.4 Server-side	20
9.5 Communication between agents and server	21
10 Privacy requirements and recommendations	22
Annex A (informative) Implementation example	24
Annex B (informative) Authentication assurance and assurance level	31
Bibliography	38

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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 27553 series can be found on the ISO website.

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

Introduction

With the fast evolution of mobile devices' capabilities in computation and functionality, authentication technologies using biometrics based on physiological or behavioural characteristics (e.g., fingerprint, face, voiceprint), have been developed and widely adopted in various mobile applications. Compared to traditional authentication methods on mobile devices such as passwords, patterns, or SMS messages, biometric characteristics are easy to use and not shareable. Since authentication methods using biometrics can provide a secure, reliable, and more convenient solution, they have become an attractive topic for both industry and academia.

However, the fragmentation of computing environments for mobile devices (e.g., different operating systems, different trusted environment implementations, different biometric system implementations, open computation environments in mobile devices, and open communication networks between mobile devices and servers) often results in inconsistent implementations, which may increase vulnerabilities and attack risks against mobile devices. This fragmentation makes it even more necessary to analyse security challenges, threats, and security frameworks for authentication using biometrics on mobile devices and to specify the high-level security requirements that could mitigate the security risks for applications of authentication using biometrics in mobile devices.

This document is the second part of ISO/IEC 27553 series, which put forward the security and privacy requirements for authentication using biometrics on mobile devices. Biometrics in this series is used for authentication using mobile devices whose result is consumed by relying parties. This document is applicable to cases where the biometric data or derived biometric data are transmitted between the mobile devices and the remote services in either or both directions. Those cases are called remote modes in this document. A typical example of remote modes is the case where biometric processing is done partially at the mobile device and partially done remotely and the result of authentication is consumed by relying parties.

Other typical examples are the cases where presentation attack detection is delegated to a remote service; where biometric reference (enrolled biometric data) is stored on an outsourced storage and sent onto mobile devices; where biometric comparison is executed within a server or distributed between mobile device and the server. Applications embodying remote modes of operation can introduce additional threats to biometric information protection and privacy compared to local modes of operation. The transmission of biometric information or storage in a server implies security and privacy threats that can be difficult to mitigate for organization with insufficient maturity level of security. Privacy threats can include:

- Eavesdropped, lost or stolen biometric data can be leveraged to forge an authentication;
- Biometric data can be exploited for identity theft in various scenarios (not limited to authentication);
- Fake biometric data can be generated based on AI tools.

This document provides high-level security requirements, taking into account that biometrics are persistent a lifetime, for authentication using biometrics on mobile devices for remote modes, including security requirements for functional components and security requirements for communication. Detailed security requirements are left to implementations. This document also analyses security challenges, threats, and security frameworks for authentication using biometrics on mobile devices.

The following contents are out of scope of this document:

- Identity proofing and enrolment using biometrics on mobile devices.
- External BPUs (Biometric Processing Unit) locally connected to mobile devices, e.g. a USB (Universal Serial Bus) key with embedded fingerprint sensor, which can be plugged into the mobile device.
- The use of biometrics for authentication to applications which are entirely local to the mobile device and no remote service is involved.
- Cases that the biometric data or derived biometric data never leave the mobile devices (see ISO/IEC 27553-1 for those cases).

Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices —

Part 2: Remote modes

1 Scope

This document provides high level security and privacy requirements for authentication using biometrics on mobile devices, in particular, for functional components, communication, storage and remote processing.

This document is applicable to remote modes, i.e., the cases that:

- the biometric sample is captured through mobile devices,
- and the biometric data or derived biometric data are transmitted between the mobile devices and the remote services in either or both directions.

The followings are out of scope of this document:

- the cases that the biometric data or derived biometric data never leave the mobile devices (i.e., local modes),
- the preliminary steps for biometric enrolment before authentication procedure, and
- the use of biometric identification as part of the authentication.

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 18031, *Information technology — Security techniques — Random bit generation*

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

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 29100:2011, *information technology — security techniques — privacy framework*

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

artefact

artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

[SOURCE: ISO/IEC 30107-1:2016, 3.1]

3.2

authentication

provision of assurance in the identity of an entity

[SOURCE: ISO/IEC 29115:2013, 3.2]

3.3

authentication agent

a component in a mobile device that performs authentication-related functions on the mobile device and interacts with the local biometric components

[SOURCE: ISO/IEC 27553-1:2022, 3.4]

3.4

entity authentication assurance

degree of confidence reached in the authentication process that the entity is what it is, or is expected to be

[SOURCE: ITU-T X.1252]

Note 1 to entry: The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

[SOURCE: ISO/IEC 29115:2013, 3.11]

3.5

authentication credential

credential containing information that can be used to help authenticate the entity.

[SOURCE: ISO/IEC 20009-4:2017, 3.3]

3.6

authentication service provider

entity that provides authentication services to a *relying party* ([3.15](#))

[SOURCE: ISO/IEC 27553-1:2022, 3.6]

3.7

biometric data

biometric sample or aggregation of biometric samples at any stage of processing, e.g. biometric reference, biometric probe, biometric feature or biometric property

Note 1 to entry: Biometric data need not be attributable to a specific individual, e.g. Universal Background Models.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.6]

3.8

biometrics

automated recognition of individuals based on their biological and behavioural characteristics.

[SOURCE: ISO/IEC 2382-37:2017, 3.1.3]

3.9 biometric processing Unit BPU

trusted implementation of a collection of biometric subprocesses implemented in a single physical unit

Note 1 to entry: A BPU commonly comprises biometric subprocesses that are sequential in the process flow for a biometric verification.

Note 2 to entry: Application/service requirements typically require BPU subprocesses to meet a uniform level of security assurance. In ACBio, assurance is achieved through a BPU evaluation process that is authenticated by means of an X.509 certificate embedded in an ACBio instance.

[SOURCE: ISO/IEC 24761:2019, 3.3]

3.10 credential

representation of an identity.

Note 1 to entry: A credential is typically made to facilitate *data* authentication of the identity information in the identity it represents.

Note 2 to entry: The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid.

EXAMPLE A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

[SOURCE: ISO/IEC 24760-1:2011, 3.3.5]

3.11 device binding

process of linking the device, the holder (individual getting the credential), and the holder data (credential)

Note 1 to entry: The binding process typically provides assurance to a known level.

[SOURCE: ISO/IEC 27553-1:2022, 3.14]

3.12 information asset

knowledge or data that has value to the individual or organization

[SOURCE: ISO/IEC 27032:2012, 4.27, modified – Note 1 removed]

3.13 mobile device

small, compact, handheld, lightweight, standalone computing device, typically having a display screen with digitizer input and/or a miniature keyboard

Note 1 to entry: Examples include laptops, tablet PCs, wearable information and communication technology (ICT) devices, and smartphones.

[SOURCE: ISO/IEC 30107-4:2020, 3.1]

3.14 presentation attack detection PAD

automated determination of a presentation *attack* ([3.19](#))

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]

3.15

relying party

RP

entity that relies on the verification of identity information for a particular entity

Note 1 to entry: A relying party is exposed to risk caused by incorrect identity information. Typically it has a trust relationship with one or more identity information authorities.

Note 2 to entry: In the context of this document (International Standard), an RP is implemented as a server plus an agent. An RP agent is a software component located in the mobile device which initiates authentication requests to an RP server, displays the returned information, and interacts with the IIP agent to fulfil the authentication process.

EXAMPLE An RP agent can be a mobile browser.

[SOURCE: ISO/IEC 27553-1:2022, 3.19]

3.16

renewable biometric reference

RBR

renewable identifier that represents an individual or data subject within a domain by means of a protected binary identity (re)constructed from the captured biometric sample, and fulfilling irreversibility requirements

Note 1 to entry: A renewable biometric reference fulfilling irreversibility requirement provides additional security property.

Note 2 to entry: An example of a renewable biometric reference is a pseudonymous identifier and additional data elements required for biometric verification or identification such as auxiliary data.

[SOURCE: ISO/IEC 24745:2022, 3.34]

3.17

threat

potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

3.18

trusted environment

secure area that guarantees the confidentiality and integrity of code and data loaded inside

Note 1 to entry: Examples include TEE (Trusted Execution Environment), SE (Secure Element), and TPM (Trusted Platform Module). See ISO 12812-1 and ISO/IEC 11889 for further details.

[SOURCE: ISO/IEC 27553-1:2022, 3.22]

3.19

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]

3.20**revocability**

ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference

Note 1 to entry: Rejection of a subject may occur on the grounds of its appearance on a revocation list.

[SOURCE: ISO/IEC 24745:2022, 3.35]

3.21**renewability**

property of a transform or process to create multiple, unlinkable transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference

[SOURCE: ISO/IEC 24745:2022, 3.33]

3.22**Biometric data subject**

individual whose individualized biometric data is within the biometric system

Note 1 to entry: The intent of the word “individualized” is to distinguish biometric data subjects from those whose aggregated data was used in the creation of the biometric recognition algorithm. Examples of individuals contributing biometric data who are not biometric data subjects include those who contributed to a Universal Background Model in speaker recognition systems, or who contributed to the creation of an eigenface basis set in a facial recognition system.

[SOURCE: ISO/IEC 2382-37:2022, 37.07.05]

3.23**biometric reference****BR**

one or more stored biometric samples, biometric templates or biometric models attributed to a *biometric data subject* (3.22) and used as the object of biometric comparison

EXAMPLE Face image stored digitally on a passport, fingerprint minutiae template on a National ID card or Gaussian Mixture Model for speaker recognition, in a database.

Note 1 to entry: A biometric reference that can be renewed is referred to as a renewable biometric reference.

Note 2 to entry: BR can be used as a factor in multi-factor authentication, that is, something a person is.

[SOURCE: ISO/IEC 24745:2022, 3.11]

3.24**biometric data controller**

person or organization which, alone or jointly with others, determines the purposes, means and goals of the processing of biometric data

[SOURCE: ISO/IEC 2382-37:2022, 37.07.26]

4 Abbreviated terms

PitM	Person-in-the-Middle
OS	Operating System
RAM	Random-Access Memory
SDK	Software Development Kit
SE	Secure Element

TEE	Trusted Execution Environment
TPM	Trusted Platform Module
BR	Biometric Reference
FAR	False Acceptance Rate

5 Security and privacy considerations

5.1 General

This document addresses the security and privacy requirements for using biometrics as an authentication mechanism in order to realize a level of authentication assurance while ensuring, by design, the security and privacy protection of biometric data. In addition to ISO/IEC 29115, Annex B in this document addresses levels of assurance.

This document considers the case of remote modes, that is where some biometric information is sent outside the mobile device. It can be the case if the relying party requests it or if the mobile device relies on some outsourced biometric service.

Possible use cases (and justification) of choosing remote modes are analysed in [5.3](#).

In addition to the challenges introduced in ISO/IEC 27553-1:2022, Clause 5, that apply also to remote modes if not specific to local modes, [Clause 5.4](#) in this document introduces security challenges that are specific to remote modes.

Taken in account these use cases and challenges, the security impact of choosing remote modes versus the local modes [ISO/IEC 27553-1] shall be assessed. The security threats shall be thoroughly considered (see [Clause 8](#)). When possible, unnecessary collection shall be avoided and local modes should be preferred.

If remote mode is strongly justified (based on risk assessment and use case constraints, see [5.2](#)), one shall comply with the security and privacy requirements in [Clause 9](#) and [Clause 10](#), in order to drastically reduce leakage and function creep risks.

NOTE The corresponding security measures are generally more easily implemented within systems with high level of security constraints/requirements.

5.2 Security challenges common to all biometric systems

Biometric systems, in general, are faced with a number of threats that may result in a vulnerability as described in [subclause 8.3](#), ISO/IEC 19792:2009, including:

- performance limitations,
- artefact of biometric characteristics,
- modification of biometric characteristics,
- difficulty of concealing biometric characteristics,
- similarity due to blood relationship,
- special biometric characteristics,
- synthesised wolf biometric samples,
- hostile environment,
- procedural vulnerabilities around the enrolment process,