



BSI Standards Publication

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

Part 1: Local modes

National foreword

This British Standard is the UK implementation of [ISO/IEC 27553-1:2022](#).

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 03715 9

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

ISO
27553-1

First edition
2022-11-02

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

Part 1: Local modes



Reference number
ISO 27553-1:2022(E)

AVA Documents
Document Sharing Hub
© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022, Published in Switzerland

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

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	5
5 Security challenges	5
5.1 General	5
5.2 Security challenges common to all biometric systems	5
5.3 Security challenges specific to authentication using biometrics on mobile devices	6
5.3.1 Diversity across mobile devices	6
5.3.2 Open computation environment	6
5.3.3 Operation in an unsupervised environment	6
6 System description	7
6.1 An example architecture	7
6.2 Entities and components	7
6.2.1 Biometric system	7
6.2.2 Relying party agent	8
6.2.3 Authentication agent	8
6.2.4 Relying party server	9
6.2.5 Authentication server	9
7 Information assets	9
8 Threat analysis	10
8.1 Threats to the biometric system	10
8.2 Threats to the authentication and relying party agents	11
9 Security requirements and recommendations	11
9.1 General	11
9.2 Biometric system	11
9.3 Mobile device	12
10 Privacy considerations	13
10.1 General	13
10.2 Privacy policy for biometric data	14
10.3 Other privacy considerations	14
Annex A (informative) Implementation example	15
Annex B (informative) Security issues related to communication between agents and servers for authentication using biometric on mobile devices	21
Annex C (informative) An example of authentication assurance and assurance levels	22
Bibliography	29

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 or www.iec.ch/members_experts/refdocs).

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 <https://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. In the IEC, see www.iec.ch/understanding-standards.

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 and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

The functionalities and computation capabilities of consumer-grade mobile devices are evolving fast. Authentication technologies using biometrics based on physiological or behavioural characteristics (e.g. fingerprint, face, voiceprint) have been developed and widely adopted across various mobile platforms. Compared to traditional authentication methods on mobile devices such as passwords, patterns, or SMS messages, biometric characteristics are easy to use and hard to share. Authentication methods using biometrics can, in some respects, provide a secure, reliable, and convenient solution, albeit with some potentially awkward restrictions.

However, the fragmentation of computing environments for mobile devices (e.g. different operating systems, different trusted environment implementations, different biometric system implementations, and open computation environments in mobile devices) often results in inconsistent implementations, which potentially increase the risks of vulnerabilities in, and attacks 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. It is also necessary to specify the high-level security requirements that can mitigate the security risks for applications of authentication using biometrics in mobile devices.

Biometrics in this document is used for authentication on mobile devices whose result is consumed by relying parties. This document applies to the cases where the biometric data and any derived biometric data, except information on the verification outcome, do not leave the device, i.e. local modes.

This document provides high-level security requirements and recommendations for authentication using biometrics on mobile devices, including for functional components and for communication between the biometric system and the mobile applications requesting authentication success. 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 not addressed in this document:

- Identity proofing and enrolment requirements.
- The use of biometrics for authentication to applications which are entirely local to the mobile device and no remote service is involved.

This page deliberately left blank

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

Part 1: Local modes

1 Scope

This document provides high-level security and privacy requirements and recommendations for authentication using biometrics on mobile devices, including security and privacy requirements and recommendations for functional components and for communication.

This document is applicable to the cases that the biometric data and derived biometric data do not leave the device, i.e. local modes.

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 24745:2022](#), *Information security, cybersecurity and privacy protection — Biometric information protection*

3 Terms and definitions

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

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

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

3.1

attack presentation classification error rate

APCER

proportion of attack presentations using the same presentation attack instrument (PAI) species incorrectly classified as bona fide presentations in a specific scenario

Note 1 to entry: PAI means the biometric characteristic or object used in a *presentation attack* ([3.17](#)).

[SOURCE: ISO/IEC 30107-3:2017, 3.2.1, modified — Note 1 to entry has been added.]

3.2

artefact

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

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

3.3

authentication

provision of assurance in the identity of an entity

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

3.4

authentication agent

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

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* ([3.19](#))

3.7

biometric data

biometric sample or aggregation of biometric samples at any stage of processing

EXAMPLE 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 2382-37:2022, 37.03.06]

3.8

biometric information

information conveyed or represented by *biometric data* ([3.7](#))

Note 1 to entry: Biometric data include for instance data derived or transformed from biometric data which are handled in connection with biometric data within a biometric system.

[SOURCE: ISO/IEC 24745:2022, 3.9]

3.9

biometric probe

biometric sample ([3.12](#)) or biometric feature set input to an algorithm for comparison to a biometric reference(s)

[SOURCE: ISO/IEC 2382-37:2022, 37.03.14, modified — Notes to entry have been removed.]

3.10

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]

3.11

biometrics

automated recognition of individuals based on their biological and behavioural characteristics

[SOURCE: ISO/IEC 2382-37:2022, 37.01.03, modified — Notes to entry have been removed.]

3.12

biometric sample

analogue or digital representation of biometric characteristics prior to biometric feature extraction

EXAMPLE A record containing the image of a finger is a biometric sample.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.21]

3.13

credential

representation of an identity for use in *authentication* (3.3)

Note 1 to entry: As described in ISO/IEC 24760-1:2019, 5.4, customary embodiments of a credential are very diverse. To accommodate this wide range, the definition adopted in this document is very generic.

Note 2 to entry: A credential is typically made to facilitate data authentication of the identity information pertaining to the identity it represents. Data authentication is typically used in authorization.

Note 3 to entry: The identity information represented by a credential can, for example, be printed on human-readable media, or stored within a physical token. Typically, such information can be presented in a manner designed to reinforce its perceived validity.

Note 4 to entry: A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

[SOURCE: ISO/IEC 24760-1:2019, 3.3.5]

3.14

device binding

association of a specific device with the data (credential) and the holder (individual getting the credential)

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

3.15

information asset

knowledge or data that has value to the individual or organization

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

3.16

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]

3.17

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 can have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: It is possible that biometric systems are unable 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, modified — "may" has been changed to "can" and "it is possible" in Notes 2 and 3 to entry.]

3.18 presentation attack detection PAD

automated determination of a *presentation attack* ([3.17](#))

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]

3.19 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, 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 identity information provider (IIP) agent to fulfil the authentication process.

EXAMPLE An RP agent can be a mobile browser.

[SOURCE: ISO/IEC 24760-1:2019, 3.3.7, modified – Note 2 to entry and EXAMPLE added]

3.20 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]

3.21 threat

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

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

3.22 trusted environment

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

Note 1 to entry: Examples include trusted execution environment (TEE), SE secure element (SE), and trusted platform module (TPM). See [ISO 12812-1](#) and the [ISO/IEC 11889](#) series for further details.