INTERNATIONAL STANDARD

ISO/IEC 27553-1

First edition
2022-11

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

Part 1: **Local modes**

Reference number
ISO/IEC 27553-1:2022(E)

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

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.

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*