ISO/IEC FDIS 27553-2~~:2025(en)~~

ISO/IEC JTC 1/SC 27

Secretariat:~~-~~ DIN

Date: 2025-~~01-29~~04-07

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

Part~~-~~ 2:
Remote modes

FDIS stage

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11

~~Fax: +41 22 749 09 47~~

~~Email~~E-mail: copyright@iso.org
Website: ~~www.iso.org~~www.iso.org

Published in Switzerland

Contents

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~~www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at ~~www.iso.org/patents and https://patents.iec.ch.~~www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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.~~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~~www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

As the computational and functional capabilities of mobile devices rapidly evolve, 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 can 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~~can mitigate the security risks for applications of authentication using biometrics in mobile devices.

This document is the second part of the ISO/IEC 27553 series, which puts forward the security and privacy requirements for authentication using biometrics on mobile devices. Biometrics in the ISO/IEC 27553 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 partially done on the mobile device and partially done remotely, and the result of authentication is consumed by relying parties.

Other typical examples include cases where:

- presentation attack detection is delegated to a remote service;
- a biometric reference (i.e. enrolled biometric data) is stored on an outsourced storage and sent onto mobile devices;
- 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:

- leveraging eavesdropped, lost or stolen biometric data to forge an authentication;
- exploiting biometric data for identity theft in various scenarios (not limited to authentication);
- generating fake biometric data 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. Further detailed security requirements are not covered here as they are implementation-dependent. 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 Biometric Processing Units (BPUs) locally connected to mobile devices, e.g. a USB key with embedded fingerprint sensor, which can be plugged into the mobile device~~.~~;
- ~~—~~—the use of biometrics for authentication to applications that are entirely local to the mobile device and no remote service is involved~~.~~;
- ~~—~~—cases where the biometric data or derived biometric data never leave the mobile devices (see ISO/IEC 27553-1 for those cases).

While identity proofing and enrolment are not covered in this document, risks and threats exist and consequently they are an integral part of the security posture of an organization relying on authentication using biometrics on mobile devices.