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*

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.

4 Abbreviated terms

BR	biometric reference
DNA	deoxyribonucleic acid
FAR	false acceptance rate
IT	information technology
PITM	person in the middle
OS	operating system
PIN	personal identification number
RTE	runtime environment
TEE	trusted execution environment

5 Security challenges

5.1 General

User authentication is done to obtain a level of trust in the identity information pertaining to that user. ISO/IEC 29115 describes different levels of assurance for the identity information obtained during authentication and specifies that biometric mechanisms can contribute to a higher level of assurance.

This document addresses the security requirements for using biometrics as an authentication mechanism in a mobile device to realize a level of authentication assurance. In addition to ISO/IEC 29115, information on levels of assurance can be found in Annex C of this document.

5.2 Security challenges common to all biometric systems

Biometric systems, in general, are faced with a number of threats that can result in vulnerabilities as described in ISO/IEC 19792:2009, 8.3 including:

- performance limitations;
- artefact of biometric characteristics;
- modification of biometric characteristics;
- difficulty of concealing biometric characteristics;
- similarity due to blood relationship;
- special biometric characteristics;
- synthesized wolf biometric samples;
- hostile environment;
- procedural vulnerabilities around the enrolment process;
- leakage and alteration of biometric data.

The components in a biometric system, and the biometric data transmitted through the interfaces between these components, confront certain threats as listed in ISO/IEC 24745:2022, Tables 1 and 2, including:

- threats to data capture: presentation attacks against the biometric capture subsystem;
- threats to signal processing: unauthorized manipulation of data during processing;
- threats to comparison: manipulation of comparison scores;
- threats to storage: database compromise;
- threats to decision: hill-climbing attack, threshold manipulation;
- threats to the interfaces between data capture, signal processing, and comparison: eavesdropping, replay, or brutal force attack on the biometric sample and feature;
- threats to the interface between storage and comparison: eavesdropping, replay, person-in-the-middle (PITM), or hill climbing attack on the biometric reference;
- threats to the interface between comparison and decision: comparison score manipulation.

Any applications depending on authentication using biometrics on mobile devices shall consider these threats and decide whether to mitigate them or accept the corresponding risks.

5.3 Security challenges specific to authentication using biometrics on mobile devices

5.3.1 Diversity across mobile devices

The IT environments of mobile devices involved in mobile transactions are diverse and variable. There is remarkable fragmentation across mobile devices, for example, different OSs, customized OS versions, different trusted environment implementations and different biometric system implementations.

Therefore, it can be more difficult to integrate all these components without vulnerabilities, even if each component is securely implemented. And it is generally harder for authentication service providers to guarantee security across environments involving a multiplicity of different mobile devices where a single party cannot manage the entire workflow.

5.3.2 Open computation environment

Unlike dedicated biometric systems, most mobile and other user-owned devices use open computation environments, for example, installable application software, which can include malware. This exposes more attack surfaces to the adversary.

Some mobile devices have a secure processing pipeline such that an operating system or kernel compromise cannot allow data to be directly injected to falsely authenticate as the user. However, if the authentication service provider can't ensure such a secure processing pipeline, this creates a significant and hard to mitigate security and privacy risk.

5.3.3 Operation in an unsupervised environment

An authentication operation on a mobile device can occur anywhere, anytime. In most cases, the authentication operation is carried out in an unsupervised environment, which can increase the risk compared to operations in supervised systems.

An unsupervised environment can facilitate presentation attacks, physical attacks on the device, and authentication attacks without the mobile device. An unsupervised environment also presents risks to enrolment as it can be difficult to ensure that the right person's biometrics is being enrolled without proper electronic verification using an identity document.

For example, when a mobile user is authenticated to log into a mobile banking system, there is no clerk over the counter to make sure it is a natural person, so presentation attacks on the biometrics-based enrolment and verification processes are more likely to happen on a mobile device than in a face-to-face scenario. Another example is unsupervised enrolment (initial authentication), which can be found in ISO/IEC TR 30125:2016, Clause 9.

6 System description

6.1 An example architecture

An example architecture for authentication using biometrics on mobile devices described in this document is shown in Figure 1. Here, the biometric subsystem is one of the subsystems shown in Figure 2. Additional information about the example architecture is provided in Annex A.

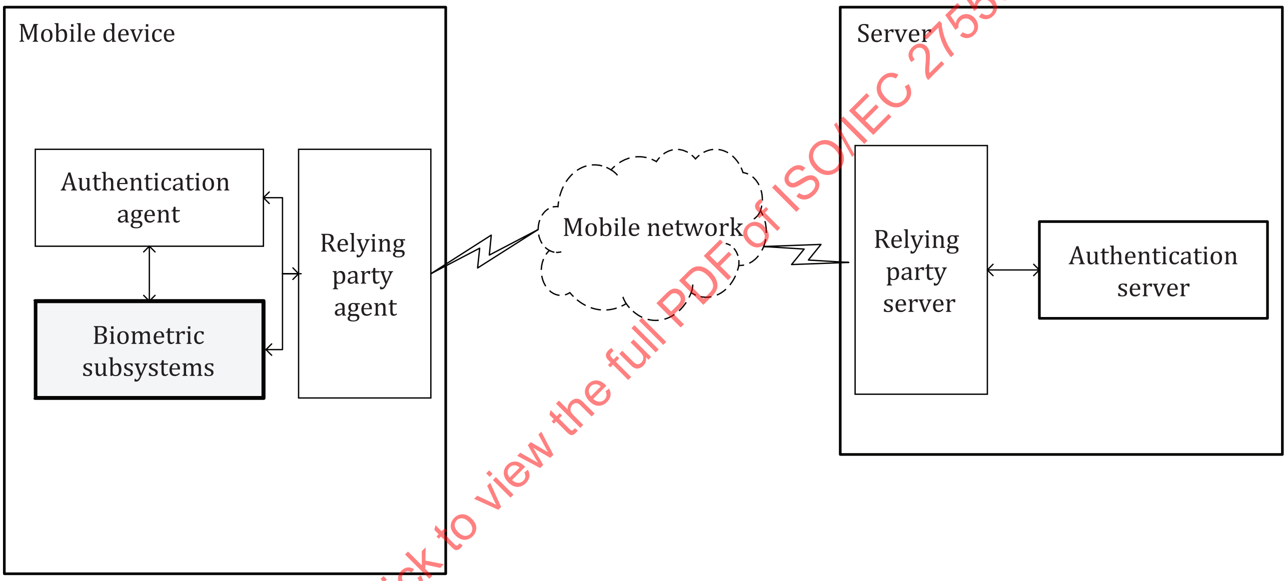


Figure 1 — Example architecture for authentication using biometrics on mobile devices

NOTE 1 The components in Figure 1 represent the logical elements of a system. Specific configurations vary across different implementations.

NOTE 2 This document focuses on the security and privacy requirements on the components in the mobile devices. Some additional security and privacy considerations are provided in Annex B for informative purposes.

6.2 Entities and components

6.2.1 Biometric system

Figure 2 is a typical architecture of a biometric system with presentation attack detection (PAD), modified from ISO/IEC 30107-1:2016, Figure 3.

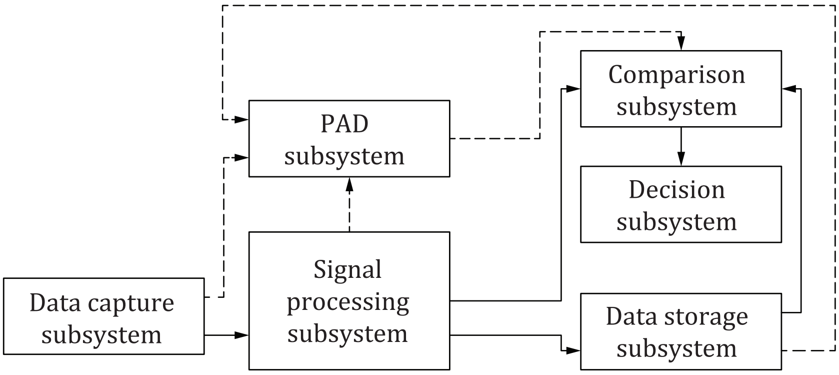


Figure 2 — Functional overview of a biometric system with PAD

The biometric system shown in Figure 2 consists of a general biometric framework and a PAD subsystem. The general biometric framework is composed of a data capture subsystem, a signal processing subsystem, a comparison subsystem, a decision subsystem, and a data storage subsystem. The PAD subsystem can be placed within the general biometric framework in a number of ways. Figure 2 shows one way by dash lines.

In this document, all of the subsystems in Figure 2 reside on the mobile device.

There are variations in practice (refer to ISO/IEC 24745 for details). The functioning of the subsystems shown in Figure 2 depends on the details of the system implementation. For example, the signal processing, comparison, and decision subsystems for a minutiae-based fingerprint system can widely differ from those for a pattern-based iris recognition system or a deep learning face recognition system. The use of renewable biometric references (RBRs) can also give rise to differences. For example, the similarity determination (comparison) process can be effectively subsumed within the signal processing subsystem, and the decision process can be deterministic like that for passwords. In addition, certain types of RBR can both conceal the subject's biometric information and also allow the generation of a credential which can be used as a key within the authentication protocol. ISO/IEC 24745:2022, Annex C, gives some examples of such RBRs.

6.2.2 Relying party agent

The relying party (RP) agent is typically provided by the relying party and installed on the mobile device. It manages communication between the mobile device and the RP server. It can include additional functionality that is beyond the scope of this document.

6.2.3 Authentication agent

The authentication agent is a component in a mobile device that performs authentication-related functions on the mobile device and interacts with the local biometric components. Although multiple authentication factors can be supported, such as passwords, PINs, tokens and biometrics, only biometrics are considered in this document.

The authentication agent interacts with the server through the RP agent. It can be a native functional component provided by the mobile device manufacturer, or a piece of installable software provided by the relying party or the authentication service provider.

In a typical implementation, the authentication agent uses authentication credentials to perform the authentication process once the biometric verification is done. In this case, the authentication agent can for instance interact with the local biometric components on the mobile device using cryptographically verifiable signed tokens.

6.2.4 Relying party server

The relying party (RP) server is responsible for providing back-end services for the RP. This includes communicating between the mobile device and server-side components like the authentication server. During the authentication process, the RP server obtains the authentication result from the authentication server and provides the corresponding service or resource according to the authentication result and the authorization policy. The RP server can include additional functionality that is beyond the scope of this document.

6.2.5 Authentication server

The authentication server performs the credential verification function during an authentication process. Upon completing the authentication process, the authentication server generates an authentication result and provides the result to the RP server. The authentication server can include additional functionality that is beyond the scope of this document.

7 Information assets

Table 1 identifies information assets to be protected and relevant objectives to be achieved, such as confidentiality, integrity, availability, authenticity/accountability, and device binding.

Table 1 — Information assets to be protected

Information asset		Security objectives	Description
Biometric system	Hardware	integrity, confidentiality, availability	The hardware of a biometric system which captures, processes, and stores the biometric data.
	Biometric data	confidentiality, integrity, renewability, revocability, privacy	Biometric sample or aggregation of biometric samples at any stage of processing. Refer to the following subclauses of ISO/IEC 24745:2022 for the description of biometric data: — confidentiality: 6.1.1 — integrity: 6.1.2. — renewability and revocability: 6.1.3. Refer to Clause 10 of this document for privacy concerns.
	Software	integrity, availability	The code of a biometric system that implements system functions and processing logic.
	Keys	integrity, availability, confidentiality, device binding	The keys managed and stored by the biometric system, e.g. encryption keys for biometric data storage or transmission, attestation keys to prove a biometric system's authenticity. Refer to ISO/IEC 24745 and ISO/IEC 24761, for details.
Authentication agent	Credentials	confidentiality, integrity, device binding	The storage and usage of user authentication credentials are performed by the authentication agent, e.g. in the trusted environment.
	Software	integrity, availability	The code of an authentication agent that implements system functions and processing logic.
	Data[a] and keys	confidentiality, integrity availability	Sensitive data and keys (e.g. encryption keys) managed and stored by an authentication agent.

[a] Only data relevant to authentication are considered in this document.

Table 1 *(continued)*

Information asset		Security objectives	Description
Relying party agent	Software	integrity, availability	The code of the relying party agent that implements system functions and processing logic.
	Data [a] and keys	confidentiality, integrity availability	Sensitive data and keys managed and stored by a relying party agent, e.g. communication keys shared with servers, or other functional components.

[a] Only data relevant to authentication are considered in this document.

8 Threat analysis

8.1 Threats to the biometric system

Threats to biometric systems have been well analysed in ISO/IEC 24745:2022, 6.2. Only high-level security considerations are provided here in Table 2.

Table 2 — Threats to the biometric system

	Threat	Description	Consequences
T.B.1	Threats against biometric system components	Refer to ISO/IEC 24745:2022, Table 1.	
T.B.2	Threats during the transmission of biometric data	Refer to ISO/IEC 24745:2022, Table 2.	
T.B.3	Presentation attacks in unsupervised environments	Refer to ISO/IEC 30107-1 and Annex C of this document.	In unsupervised operating environments, attackers can implement presentation attacks to spoof the biometric system for successful authentication.
T.B.4	Fake biometric system	The biometric system or subsystems, as a whole or partly, are replaced with a fake one in a mobile device.	With a fake biometric system, attackers can acquire a user's biometric data or output bogus biometric verification results.
T.B.5	Key leakage	The keys managed and stored by the biometric system are revealed to the attackers or reused on another device.	The data protected by the keys are revealed. Or the attributes (e.g. a biometric system's authenticity) associated with the key are compromised.
T.B.6	False match	False match decisions	Incorrect authentication results.
T.B.7	Exposure of Recovered key	The BPU runtime is attacked to gain access to the recovered key.	Same as T.B.5 Only applicable to RBR implementations where the authentication key is recovered from a matching biometric capture.

8.2 Threats to the authentication and relying party agents

Threats to the authentication and relying party agents include those listed in Table 3.

Table 3 — Threats to the authentication and relying party agents

	Threat	Description	Consequences
T.M.1	Malicious relying party agent	Compromises can include: a) undeclared relying party agent app functionality; b) infection of the relying party agent app with trojans, viruses, etc; c) vulnerabilities of the relying party agent app code or functionality that can provide an attack vector facilitating subsequent attacks on the user device.	A compromised agent can damage the mobile device's software and hardware and be used to steal user data, including personal data, monitor user activity, expose the device and data to future attacks, etc.
T.M.2	Malicious authentication agent	Compromises can include: a) undeclared authentication agent app functionality; b) infection of the authentication agent app with trojans, viruses, etc; c) vulnerabilities of the authentication agent app code or functionality that can provide an attack vector facilitating subsequent attacks on the user device.	A compromised agent can damage the mobile device's software and hardware and be used to steal user data, including personal data, monitor user activity, expose the device and data to future attacks, etc.
T.M.3	Authentication agent corruption	The agent malfunctions due to software or hardware issues.	Disrupting the availability of the authentication agent.
T.M.4	Extracting credentials from the device	Stealing the credentials stored in the mobile device and using them on other devices.	Attackers can impersonate the user and succeed in authentication with the leaked credentials.
T.M.5	Bypassing access control of credentials	Unlocking the credentials in the device without the associated user biometric verification process.	Attackers can impersonate the user for authentication from the same mobile device without user consent.
T.M.6	PITM attack between agents	Eavesdropping or modifying the messages between the relying party agent and the authentication agent.	An attacker can intercept and possibly modify authentication messages between agents to convince the agents that they are communicating with a legitimate user.

9 Security requirements and recommendations

9.1 General

This clause provides high-level security requirements and recommendations for authentication to remote services using biometrics on mobile devices. These requirements and recommendations are categorized according to the architecture, as in Figure 1.

9.2 Biometric system

Minimal security requirements and recommendations for the biometric system are described in Table 4.

Table 4 — Security requirements and recommendations for biometric system

	Requirements and recommendations	Threats to be mitigated
SR-B-1	Countermeasures defined in ISO/IEC 24745:2022, 6.2.1, shall be adopted to protect the assets in a biometric system.	T.B.1 T.B.2 T.B.3 T.B.7
SR-B-2	Countermeasures defined in ISO/IEC 24745:2022, 6.2.2, shall be adopted to protect the assets during the transmission of biometric data between the various components (subsystems) of the biometrics system.	
SR-B-3	Biometric information shall not leave the mobile device.	
SR-B-4	For applications where a very high level of authentication assurance is necessary, the biometric system should have the ability to detect hardware intrusion and to delete the sensitive data and keys if hardware intrusion is detected.	
SR-B-5	Biometric information shall be securely deleted from the mobile device when no longer needed.	
SR-B-6	The authenticity and integrity of the biometric system shall be verified, e.g. verify that it is digitally signed by a trusted provider.	T.B.4
SR-B-7	The keys in the biometric system shall be protected from being revealed or reused on another device.	T.B.5 T.B.7
SR-B-8	The biometric comparison should be performed in an isolated execution environment, such as the trusted environment.	General
SR-B-9	All biometric information should be encrypted and cryptographically authenticated such that they cannot be acquired, read, or altered outside an isolated execution environment, such as the trusted environment.	General
SR-B-10	Access to unencrypted biometric information outside an isolated execution environment, such as the trusted environment, should not be allowed.	General
SR-B-11	Biometric systems should perform at or above internationally recognized minimum performance guidance, for example, the guidance in ISO/IEC TR 29156, and the testing frameworks in ISO/IEC 30107-3 and ISO/IEC 19795-1.	T.B.3 T.B.6
SR-B-12	The security of the biometric systems should be assessed and go through a security audit. For example, see either ISO/IEC 19792 or ISO/IEC 19989 as a reference for biometric system security evaluation.	General

9.3 Mobile device

The mobile device security requirements and recommendations listed in Table 5 are the countermeasures to mitigate the non-biometric threats against mobile devices.

Table 5 — Security requirements and recommendations for mobile device

	Requirements and recommendations	Threats to be mitigated
SR-M-1	All security assets in a mobile device shall be protected commensurate with their security properties, as indicated in Clause 7.	General
SR-M-2	The mobile device operating system should not be customized and shall be securely updated to the latest secure version.	
SR-M-3	The development process of the relying party agent and the authentication agent shall apply secure design and secure coding practices. For example, see the ADV class in ISO/IEC 15408-3:2008 as a reference for secure design.	T.M.1 T.M.2 T.M.3

Table 5 *(continued)*

	Requirements and recommendations	Threats to be mitigated
SR-M-4	The relying party agent and the authentication agent shall be securely verified before installation, e.g. agent installation package code signature verification.	T.M.1 T.M.2
SR-M-5	There shall be a secure binding of the relying party agent and the authentication agent with the mobile device once the agents are installed.	
SR-M-6	The relying party agent and the authentication agent shall be protected against unauthorized modification or update.	T.M.3 T.M.4
SR-M-7	The integrity of the relying party agent and the authentication agent shall be verified at runtime.	
SR-M-8	The relying party agent and the authentication agent shall not run in debug or test mode except during the development process.	
SR-M-9	Code and data protection should, where appropriate, be enhanced against reverse engineering in the relying party agent and the authentication agent, e.g. attestation, obfuscation, or white-box crypto.	
SR-M-10	The authentication agent should be protected in a trusted environment.	
SR-M-11	The user credentials in the mobile device shall be protected from unauthorized access without passing associated biometric or knowledge-based (e.g. a recovery PIN or key) verification.	T.M.4 T.M.5
SR-M-12	If the relying party agent, the authentication agent, or the servers detect any compromise, the agents shall support the capability to be deactivated or to remove all sensitive data and keys securely.	T.M.3 T.M.4
SR-M-13	If any compromise of the relying party agent and the authentication agent is detected, a capability to report it to the servers for remedial action shall exist.	
SR-M-14	The relying party agent and the authentication agent shall have the ability to identify the identity of communication counterparties and their authorized privileges.	T.M.6
SR-M-15	The communication between the agents shall be protected from PITM attacks.	
SR-M-16	Random numbers shall have sufficient entropy and should not be predictable as defined in ISO/IEC 18031.	
SR-M-17	There should be a secure processing pipeline such that an operating system or kernel compromise cannot allow data to be directly injected to falsely authenticate as the user, if not already overcome by other means.	General
SR-M-18	There shall be a secure processing pipeline such that an operating system or kernel compromise cannot allow biometric data to be extracted from the biometric system.	General

10 Privacy considerations

10.1 General

This clause provides high-level privacy considerations for authentication using biometrics on mobile devices. Two major roles are considered in such system:

- biometric data subject: the individual whose biometric data are processed in the concerned system;
- biometric data controller: the entity that gathers and controls the biometric data in the concerned system.

10.2 Privacy policy for biometric data

The biometric data controller should define a privacy policy for biometric data, including but not limited to:

- information about the biometric data controller, including the identity, the contact information, etc.;
- the service functions that collect and use the biometric data and the types of biometric data they collect, respectively (note that any sensitive personal information should be highlighted);
- the rules for handling biometric data, e.g. collecting method, storage period, etc.;
- the biometric data subject's rights and how to ensure them, e.g. how to query, correct, delete, deregister, withdraw an authorization, obtain a copy, or make a complaint about biometrics;
- the privacy risks of providing biometric data, and the consequences of not providing biometric data;
- the measures taken to protect biometric data and other personal information;
- information about how to handle a biometric data subject's query and complaint, as well as the dispute resolution institution and its contact information;
- an inventory of privacy sensitive information or data.

The content of a privacy policy should be clear and easy to understand, use common language in the concerned jurisdiction, use standard notation for figures, diagrams, etc., and avoid ambiguous expressions.

The privacy policy should be made readily available to all members of the user community, for example, on a website's homepage or on the installation start-up page of a mobile application.

The privacy policy should be delivered to each of the concerned biometric data subjects. When delivering the privacy policy to the biometric subjects, it should be converted into a privacy notice based on ISO/IEC 29100. If the cost is too high or there is obvious difficulty in fulfilling this requirement, at least it should be published as a public announcement. The content of the privacy policy should be brought to the attention of the biometric data subjects prior to their first use of the product/service. Relevant support should be available to help them to understand the privacy policy upon their first sign-up to a biometric related product or service, to help them understand the scope (e.g. purpose of use) and rules (e.g. user consent) of biometric data handling for this product or service, in order to allow the biometric data subject to decide whether to proceed.

If the information contained in a privacy policy changes, the privacy notice should be updated and delivered to the biometric data subjects in a timely manner.

10.3 Other privacy considerations

The following ISO/IEC standards should also be considered when implementing authentication using biometrics on mobile devices (local modes):

- A formal risk assessment process should be carried out in accordance with ISO/IEC 29134.
- User consent for the collection, storage, and processing of personally identifiable information (PII) should be obtained in accordance with ISO/IEC 29184.
- Appropriate privacy protection controls and mitigation measures should be implemented in accordance with ISO/IEC 29151 and ISO/IEC 24745.
- Regular privacy audits should be conducted in accordance with recognized standards such as ISO/IEC 27007 and ISO/IEC 27701.

Annex A
(informative)

Implementation example

A.1 General

This annex provides additional information about the example architecture in 6.1.

NOTE The protocol descriptions are simplified and do not address the handling of failure conditions.

A.2 Example architecture

Biometric processing is done entirely in the mobile device. A successful match of the biometric probe of the data subject releases the user authentication credential from the mobile device for transmission to the server for onward authentication on the server. Figure A.1 illustrates a typical implementation.

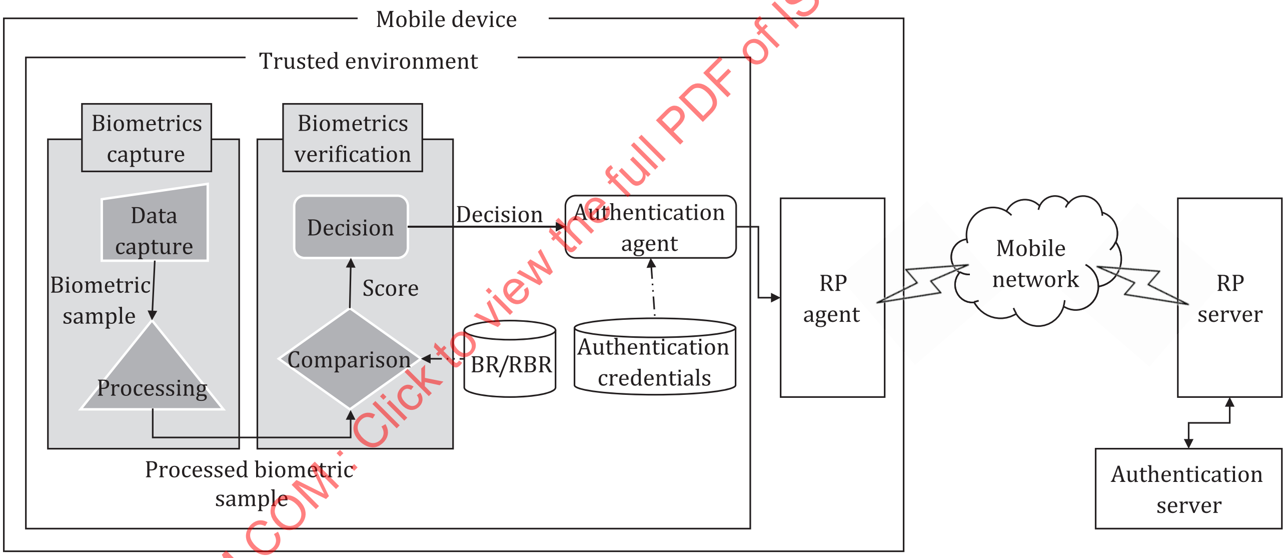


Figure A.1 — Typical implementation

Figure A.2 illustrates a variation of Figure A.1 using a renewable and revocable biometric reference instead of a typical unprotected biometric reference. Figure A.2 illustrates, more particularly, the recovery of credentials from the computation of RBR and biometric capture.

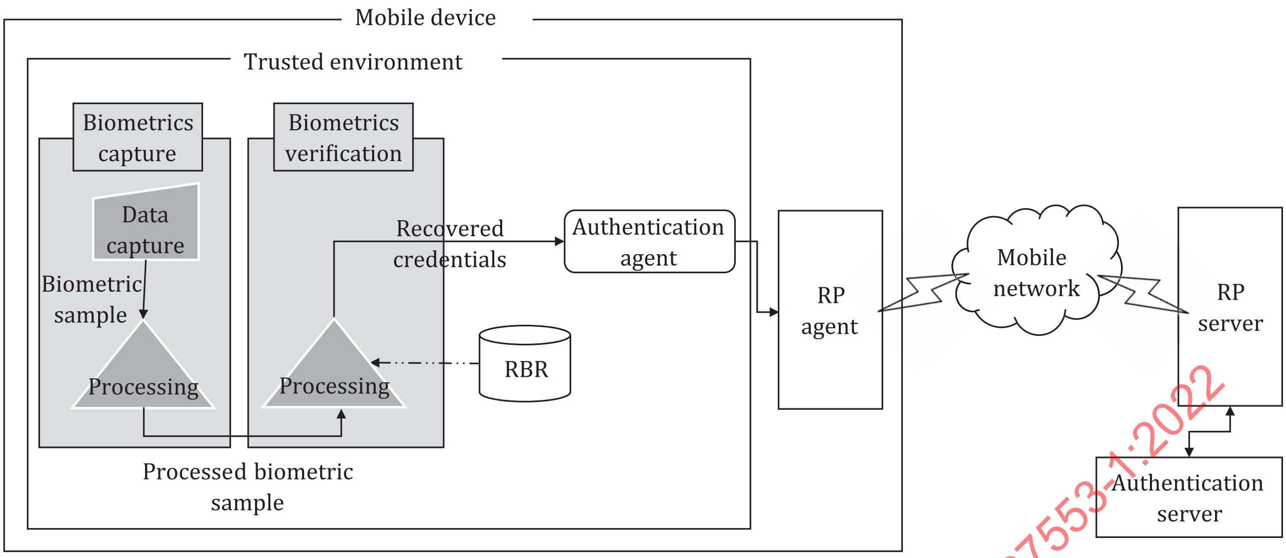


Figure A.2 — Recovering authentication credentials from RBR

A.3 Typical business processes

A.3.1 Overview

The basic idea is to decouple the local biometric verification process from remote server authentication. Typical business processes include registration, authentication, and deregistration.

Registration is the process for users to establish an authentication relationship with the service provider. Although identity proofing and enrolment are not included in the scope of this document, a successful registration is regarded as the pre-condition to implement the technical solutions described in this document.

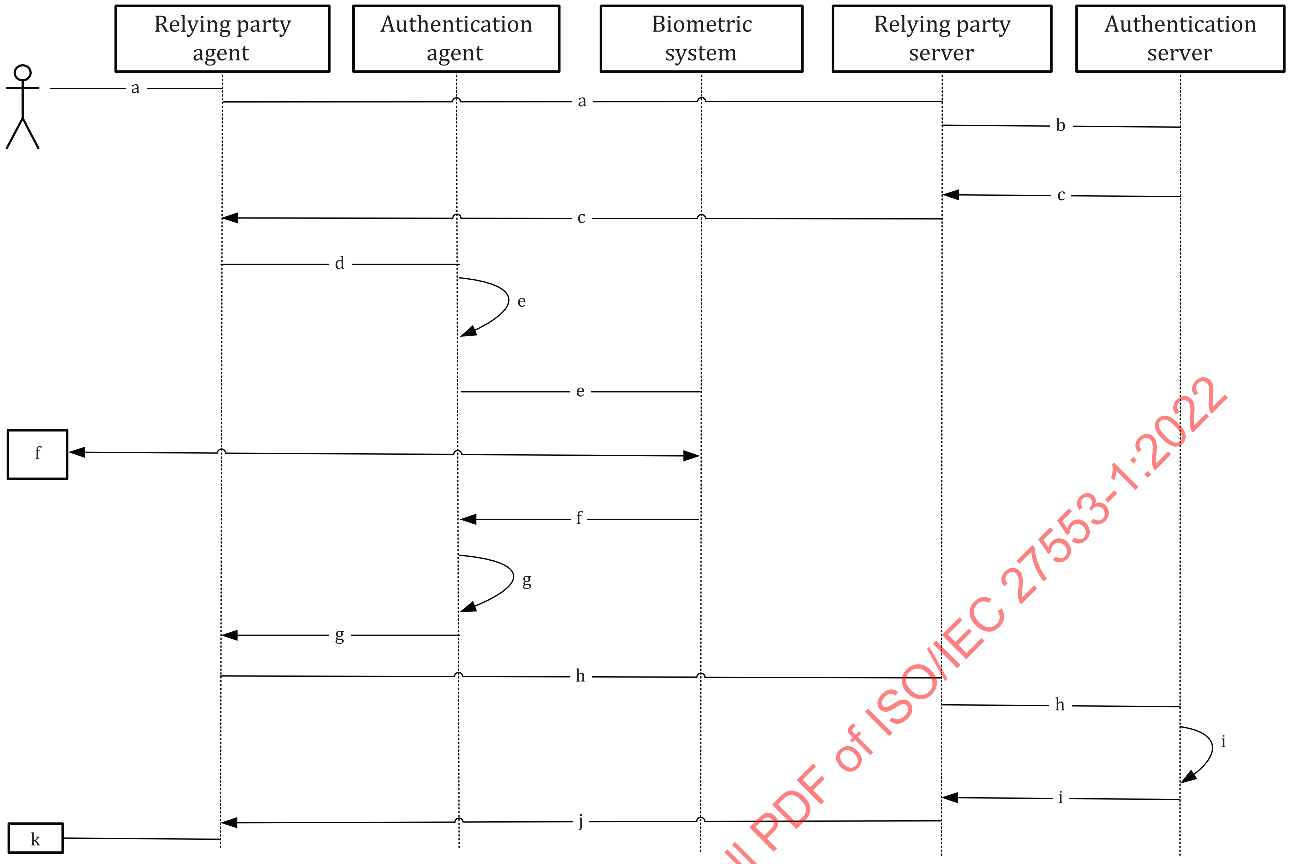
Registration process involves generating user authentication credentials in the mobile device and associating the usage of the credentials with a biometric verification process. In the following example, the integrity of the user authentication credential is protected by means of digital certificate associated with a key pair generated by the mobile device based on asymmetric cryptography. The private key is stored securely in the mobile device and managed by the authentication agent. The public key is registered in the authentication server and used in the authentication process. A public key identifier (or identity document) is recorded on the mobile device which is used in the authentication process to fetch the registered public key associated with the user.

Authentication is the process to authenticate a user based on the established authentication relationship and registered credentials. Authentication process is the main topic of this document. When a user requests authentication from a relying party agent for some business operations such as authorizing a transaction, the user first undergoes an associated biometric verification process to unlock the usage of the private key in the credential to sign some dynamic data related to the operation. Then the relying party agent sends the signed data block and the public key identifier (or the identity document) to the authentication server through the relying party server. The authentication server uses the corresponding public key to verify the signature and then returns an authentication result to the relying party server.

Deregistration is the process for users to deregister the authentication credentials. This process involves deleting all the related authentication credentials on the remote authentication server and optionally on the mobile device.

A.3.2 Registration

The message flow of registration is presented in Figure A.3.



[a] The user initiates registration through the relying party agent on a mobile device, and a registration request message is sent to the relying party server.

[b] The relying party server checks whether the registration request message is legitimate, and if legitimate, forwards it to the authentication server.

[c] The authentication server checks whether the registration request message is legitimate, and if legitimate, returns a registration challenge message to the relying party agent through the relying party server.

[d] The relying party agent calls the interface provided by the authentication agent and sends the registration challenge message to the authentication agent.

[e] The authentication agent checks whether the registration challenge message is legitimate, and if legitimate, calls the biometric system to trigger the biometric verification process if the user has enrolled, or the biometric enrolment process if the user has not enrolled.

[f] The biometric system processes the user biometric verification or enrolment operation and returns the process result to the authentication agent and the user.

[g] The authentication agent randomly generates user credentials (i.e. an asymmetric key pair) and binds with the biometric verification process. Then the authentication agent generates a registration response message including the authentication credential (i.e. the public part of the asymmetric key pair) and other related data elements (e.g. associated biometric reference identifier), and returns the registration response message to the relying party agent.

[h] The relying party agent forwards the registration response message to the authentication server through the relying party server.

[i] The authentication server verifies the registration response message, and if the verification passes, registers the authentication relationship and stores the corresponding user credential in the credential manager, then returns a registration result message to the relying party server.

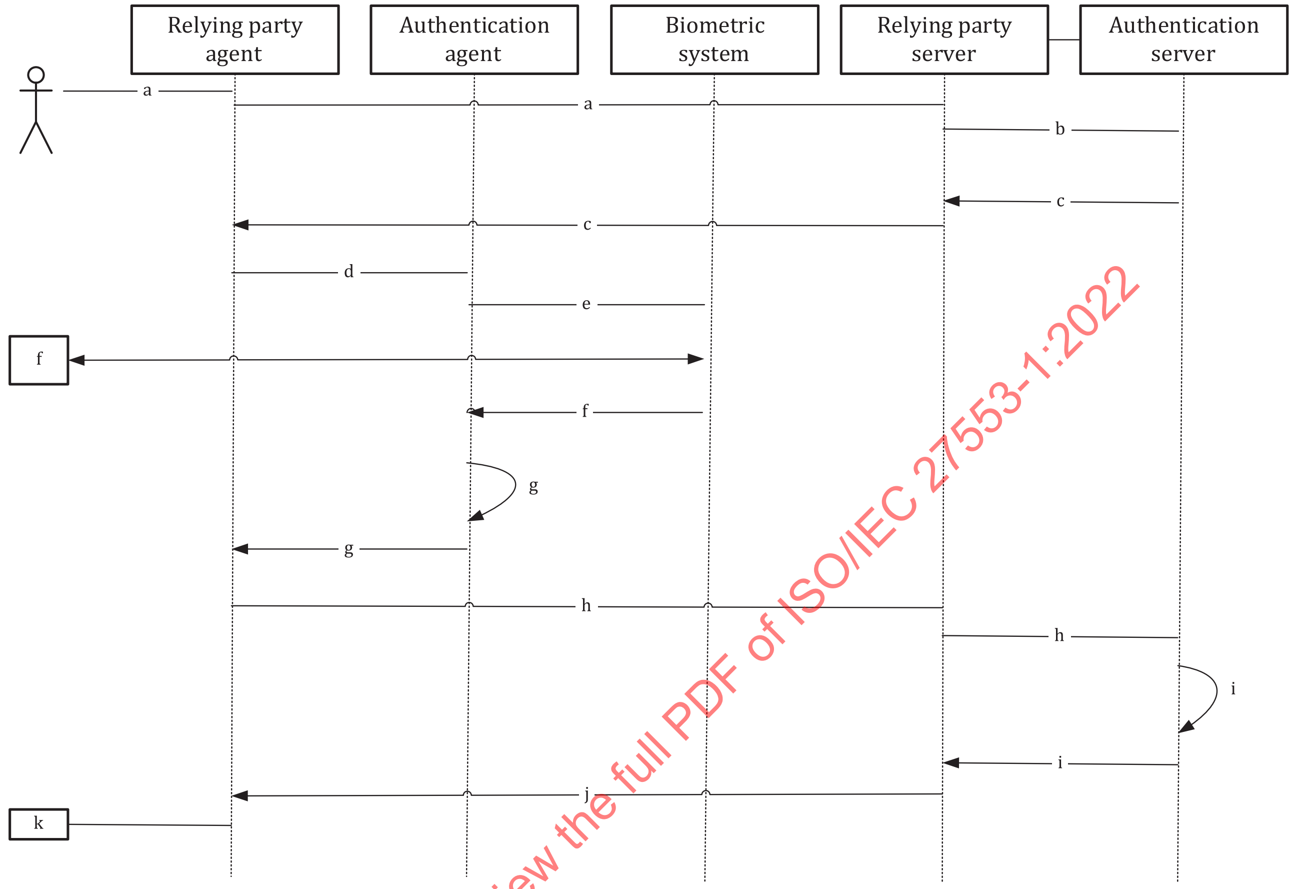
[j] The relying party server returns the registration result to the relying party agent.

[k] End of the registration process.

Figure A.3 — The message flow of registration

A.3.3 Authentication

The message flow of authentication is presented in Figure A.4.



[a] The user initiates authentication through the relying party agent on a mobile device, and an authentication request message is sent to the relying party server.

[b] The relying party server checks whether the authentication request message is legitimate, and if legitimate, forwards it to the authentication server.

[c] The authentication server checks whether the authentication request message is legitimate, and if legitimate, returns an authentication challenge message to the relying party agent through the relying party server.

[d] The relying party agent calls the interface provided by the authentication agent and sends the authentication challenge message to the authentication agent.

[e] The authentication agent checks whether the authentication challenge message is legitimate, and if legitimate, calls the associated biometric system for the biometric verification process.

[f] The biometric system processes the user biometric verification operation and returns the process result to the authentication agent.

[g] If the user successfully passes the biometric verification process, the authentication agent uses the private part of the user credential to sign the authentication data to generate an authentication response message. The authentication agent returns the authentication response message to the relying party agent.

[h] The relying party agent forwards the authentication response message to the authentication server for verification through the relying party server.

[i] The authentication server retrieves the registered authentication relationship associated with the specified public key identifier (or the identity document) and verifies the signature of the authentication data in the authentication response message. Then the authentication server generates an authentication result message and sends it to the relying party server.

[j] The relying party server returns the authentication result to the relying party agent and the user.

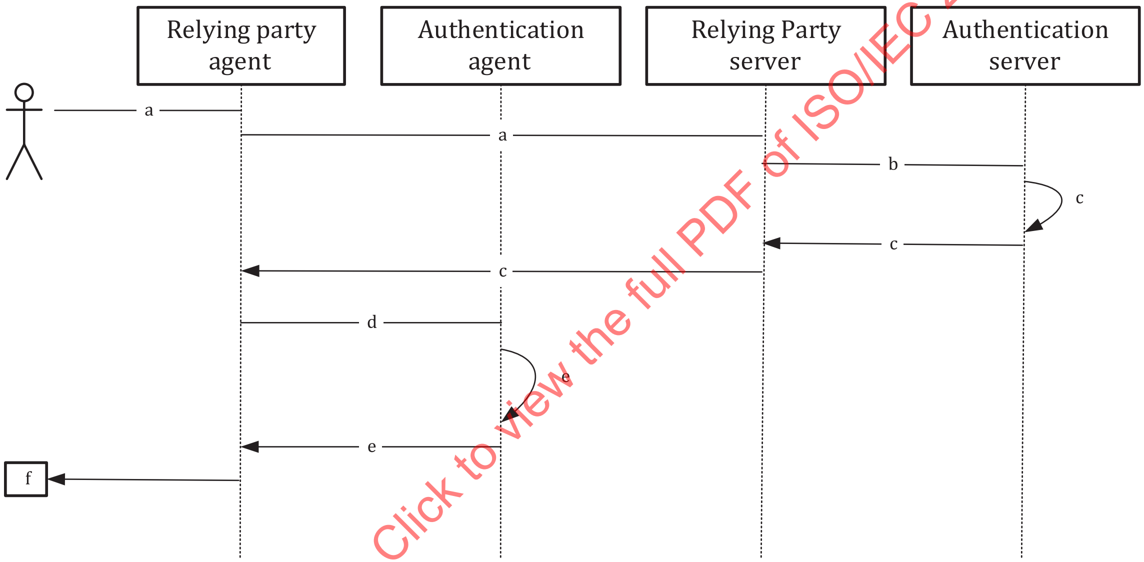
[k] End of the authentication process.

Figure A.4 — The message flow of authentication

A.3.4 Deregistration

Deregistration can be initiated by the relying party server or by the user. Server-initiated deregistration can be done without interactions between the server and the user.

The message flow of user-initiated deregistration is presented in Figure A.5.



[a] The user initiates deregistration through the relying party agent on a mobile device, and a deregistration request message is sent to the relying party server.

[b] The relying party server checks whether the deregistration request message is legitimate, and if legitimate, forwards it to the authentication server.

[c] The authentication server checks whether the deregistration request message is legitimate, and if legitimate, deletes the corresponding authentication relationship from the register and remove the associated user credentials from the credential manager. The authentication server then returns a deregistration result message to the relying party agent through the relying party server.

[d] The relying party agent calls the interface provided by the authentication agent and sends the deregistration result message to the authentication agent.

[e] The authentication agent processes the deregistration result message locally, including identifying and deleting the authentication relationship and all the associated user credentials in the mobile device. Then the authentication agent returns the processing result to the relying party agent and the user.

[f] End of the deregistration process.

Figure A.5 — The message flow of deregistration

Annex B
(informative)

Security issues related to communication between agents and servers for authentication using biometric on mobile devices

B.1 General

This annex provides additional information about the security issues related to communication between agents and servers which is part of the example architecture in 6.1 and the business processes in Annex A.

B.2 Threats to communication between agents and servers and mitigations

The threats to communication between the agents and servers are described in Table B.1.

Table B.1 — Threats to communication between agents and servers

	Threat	Description	Consequences
T.C.1	PITM attack	Attackers position themselves between the authentication agent and the authentication server so they can intercept and alter the content of the authentication protocol messages.	Attackers can implement successful user impersonation or a server impersonation attack.
T.C.2	Replay attack	Attackers capture authentication messages from a legitimate user to a server and replay them afterwards to be authenticated as the legitimate user.	Attackers can implement successful user impersonation attacks.
T.C.3	Bogus/phishing server	A bogus/phishing server is created to persuade an unsuspecting mobile user to interact with the server believed to be genuine.	Confidential or private information can be revealed. In some cases, financial loss can happen due to fraudulent transactions.

Possible mitigations for these threats are listed in Table B.2.

Table B.2 — Threat mitigations for communication between agents and servers

	Security measures	Threats to be mitigated
SR-C-1	All security assets transmitted in the communication channel between agents and servers can be protected commensurate with their properties defined in Clause 7.	General
SR-C-2	The agents or servers can have the ability to identify the identity of communication counterparties, e.g. using TLS certificates.	
SR-C-3	The communication between the agents and servers can be protected against PITM attacks.	T.C.1
SR-C-4	The communication between the servers can be protected against replay attacks, e.g. using dynamic data in protocol messages such as nonce, challenge, or timestamp.	T.C.2
SR-C-5	Mutual authentication can be enabled between the agents and the servers, if not already overcome by other means.	T.C.3

Annex C
(informative)

An example of authentication assurance and assurance levels

C.1 Introduction

C.1.1 General

This annex provides a method to evaluate how much confidence can be put in an implementation which claims to have fulfilled the requirements and followed the recommendations specified in the main body of this document.

C.1.2 Considerations for authentication assurance

A notable strength of biometric authentication is the property of inherence which bestows strong binding of biometric characteristics to users. This is different from authentication by passwords or tokens where the user is indirectly authenticated by inference, and the confidence in the authentication is limited by the strength of binding the password or token to the user.

The confidence that mobile authentication with a biometric decision is correct is ultimately limited by the technical strength of the security of the underlying authentication and biometric mechanisms. However, the confidence can be further limited by:

- vulnerabilities related to implementation choices and associated devices, together with the ease/difficulty of exploitation;
- human and procedural weaknesses associated with the authentication process;
- the strength of binding between the authentication credential and the user;
- risks remaining after threat mitigation measures are employed.

The use of biometrics on a mobile device for authentication can be implemented in different ways:

- Architectures: Different architectures can be subject to different threats.
- Security level of the critical components: which means different risk levels across different implementations.
- Biometric modalities: Considering mobile authentication, different biometric modality can be subject to different threats.
- Selection of biometric subsystem: different products can be subject to different threats.

Mobile devices are not under the control of the relying party. This makes it difficult to establish trust and assurance for user transactions. In this scenario, proof keys can be used to convey trustworthy indicators of the results of previous evaluation, testing and certification procedures for the biometric recognition technology employed and the overall system implementation. Proof keys typically involve cryptographically based digital certificates, which can be embedded within transactions to convey trust indicators that a genuine subsystem has been used for the required purpose along with parameters and appropriate assurance levels.

C.1.3 Assurance levels

Assurance levels are an expression of confidence in the biometric authentication result. Such confidence depends on both the security of the underlying system and mitigation of the threats described in C.1.1. More particularly, the assurance levels result from the ranking of threat mitigations applicable to the implementation of the security requirements defined in the specification. This annex considers a ranking of threat mitigations for biometrics and for the underlying system, which is necessary to understand the quality of the biometric modality.

The assurance level for authentication using biometrics on a mobile device is a vector, based on the false acceptance rate (FAR), presentation attack detection (PAD), threat mitigations on authentication credentials, biometric modality and data, and proof keys.

C.1.4 Achieving the required level of authentication assurance

The controls described elsewhere in this document provide a means of achieving and maintaining the required level of authentication assurance, considering operational performance limitations and technical and human/procedural vulnerabilities.

The security requirements for the mobile device in Table 5 provides countermeasures to the threats identified in Tables 2 and 3. Implementation of such requirements can be ranked according to the selected mitigations.

Table C.1 categorises threat mitigations applicable to identified threats. The mitigation categories are then addressed in more detail in C.2 and C.3

Table C.1 — Threat mitigations supporting mobile and biometrics security requirements

Security requirements	Threat mitigation categories
SR-M-1, SR-M-2, SR-M-3, SR-M-4, SR-M-5, SR-M-6, SR-M-7, SR-M-8, SR-M-9, SR-M10, SR-M12, SR-M-13, SR-M-14, SR-M-15, SR-B-3, SR-B-4, SR-B-5, SR-B-6, SR-B-7	Threat mitigations that can be conveyed only by the strength of the proof or strength of a signature key to prove the mobile application is genuine and follows the security recommendations.
SR-B-1, SR-B-2, SR-B-7	Threat mitigations that depend on the processing of the biometric reference or capture.
SR-M-10, SR-M-11, SR-B-7	Threat mitigations on the authentication credentials.
SR-B-1, SR-B-2	Threat mitigations related to presentation attacks external to the mobile device, i.e. independent from PAD and FAR.
SR-M-15, SR-M-16, SR-B-3	Threat mitigations related to the strength of cryptography (random numbers, key size, algorithm, etc.).

A security evaluation can be employed to confirm that the required level of assurance is met by a mobile device-based biometric authentication system.

C.2 Mitigation of the threats of acquiring biometric data for use in mounting presentation attacks

C.2.1 General

Presentation attack instruments (PAIs) can be created from biometric data acquired directly from a targeted subject (e.g. photograph of face, latent fingerprint etc.) or from biometric data processed or stored in a biometric system. The easier to acquire a usable biometric reference, the higher the risk of presentation attack. Appropriate choices can mitigate that risk and improve assurance level that the authentication is genuine.

The success of such kind of attack depends for most in the strength of the PAD of the biometrics system. PAD is covered in detail in the ISO/IEC 30107 series.

C.2.2 Threat mitigation by transformation of the BR and BP

According to ISO/IEC 24745, different transformation methods are available to encode the biometric reference (BR) or biometric probe (BP). Transforming the biometric into a format unusable for recovering biometric data allows to mitigate the threat of preparing a presentation attack.

Threat mitigations are considered as in Table C.2.

Table C.2 — Mitigation of threats to the biometric data

Criteria		Rating for each criterion		
		Strength level 1	Strength level 2	Strength level 3
B1	Transformation of BR	No transformation [a]	Irreversible transformation [b]	Renewable transformation [c]
B2	Transformation of BP			

[a] Highest risk: can be used to create a fake to impersonate someone.

[b] Medium risk: can be used on compromised biometrics system without recovery.

[c] Low risk: can be revoked if compromised, fraud detection pending signature verification on back-end.

C.2.3 Threat mitigation against preparation of presentation attack

The quality of the PAD takes care of presentation attacks. However, the PAD subsystem can be under different stress level depending on the relative easiness to acquire information to prepare such kind of attack.

The choice of modality can affect the difficulty of direct acquisition. Acquisition of biometrics usable to prepare an attack is a threat that can be mitigated based on multiple criteria presented in Table C.3:

- from any distance e.g. camera;
- without the presence of the user to attack e.g. DNA, fingerprints marks;
- without awareness of the user to attack e.g. capture performed without the need for the user to voluntarily present his/her biometrics on a sensor.