TECHNICAL REPORT

ISO/IEC TR 30125

First edition
2016-05-01

Information technology — Biometrics used with mobile devices

Technologies de l'information — Biométrie utilisée avec des appareils mobiles

Reference number
ISO/IEC TR 30125:2016(E)

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

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 37, *Biometrics*.

Introduction

The widespread use and capability of mobile technology has created a demand for people to be able to conduct their personal and business lives on the move in a way that previously would have been limited to the home and office environments. To service this demand, mobile communications, applications and transactions need to be protected to safeguard the privacy of the user and to ensure the integrity of the transaction. This is essential for creating a trusted mobile platform environment in which individuals, businesses, non-profit organizations and governments can transact. User authentication, being sure that you are dealing with the right person, is a vital part of this and one that poses particular difficulty when the user is communicating from an unknown remote location. The potential for impersonation and fraud is high.

User authentication is commonly achieved through the use of a username and password. This approach uses only one category of credentials, the password, and is referred to as Single Factor Authentication (SFA). Use of a biometric instead of a password is another example of SFA. For mobile applications that require high levels of security, policy may require the use of more than one credential. Use of more than one credential is referred to as Multi Factor Authentication (MFA). Multi-factor authentication can be accomplished with one or more of the following:

a) something you know (e.g. password);

b) something you have (e.g. identity card);

c) something you are (e.g. face, fingerprints, iris).

Authentication, in providing assurance that a person is who they say they are, can be improved through the use of biometric recognition. Other forms of identification, such as tokens or passwords, are not closely bound to an individual in the same manner as a biometrics is, and provide greater opportunity for substitution or theft. Password and token authentication authenticates the password or the token not the person and the authentication assurance is limited by the level of trust that exists that the password or token is being presented by the legitimate user and has not been acquired by an impostor.

The range of mobile devices and communication channels involved in mobile transactions is large and variable. Smart phones, tablets, laptops and other smart devices based on embedded systems are common examples of mobile devices and the Internet and Global System for Mobile communications (GSM) are examples of communication channels. Mobile devices are often owned by their users but not always; they could be company owned and supplied to employees for their own use.

A number of mobile device manufacturers produce units containing sensors. Conceivably, these sensors could be used to collect biometrics [i.e. camera for face, touch screen for finger or palm, microphone for voice, Global Positioning System (GPS) and accelerometers for gait]. Applications built for mobile platforms may use these sensors to capture biometrics for purposes such as authentication.

This Technical Report addresses the use of biometrics in scenarios where a person is mobile and wants to connect to a specific service irrespective of the device type and communication channel.

There are three key issues to consider when biometrics are used in such scenarios.

— The biometric capture environment – application developers will require a means of taking into account the uncontrolled nature of the capture environment. The uncontrolled capture environment will most likely mean that it is not possible for capture conditions to conform to the 'best practice' constraints for biometric capture (e.g. pose, background, etc.) set out in current biometric standards; and also require recognition algorithms and/or thresholds to be modified to take account in the case of reduced quality of biometric capture if the application can be compliant with reduced security.

— Biometric data privacy and security implications – the distribution of biometric data to commercial devices with security weaknesses and storage of biometric data in third-party cloud implementations. In this Technical Report, these security and privacy issues are addressed by referencing other standards where available noting that work is ongoing in establishing benchmarks and 'best

practice' to safeguard information including personal information. Definition of standards for security in mobile devices is not in the scope of this Technical Report.

— Biometric authentication - relative consistency of approach to biometric authentication across all application developers to ensure 'best practice' and consistent 'look and feel' for users." (More information may be found in NISTIR 8003).

Current biometric standards and associated security standards for biometrics do not yet adequately address the issues raised with the use of biometric capture on commercial computing devices, with distribution of biometric data via 'the cloud'. Work is still required in establishing benchmarks and 'best practice'.

This Technical Report is aimed at all parties with an interest in offering biometric functions or a biometric framework for use on mobile platforms including developers of third-party open source software libraries. It is also intended to provide a reference document for standards developers seeking to develop standards for the use of biometrics in mobile environments.

Information technology — Biometrics used with mobile devices

1 Scope

This Technical Report provides guidance for developing a consistent and secure method of biometric (either alone or supported by non-biometric) personalization and authentication in a mobile environment for systems procured on the open market.

Guidance is provided for

— 1:1 verification or 1:few positive identification;

— biometric sample capture in the mobile environment where conditions are not well controlled and not covered in ISO/IEC Biometric interchange format standards and the ISO/IEC Biometric sample quality Technical Reports;

NOTE 1 Further information regarding architectures may be found in NIST/SP 500-288.

— the best use of multiple biometric and non-biometric (PINs, passwords, personal data) personalization and authentication methods (i.e. multifactor).

NOTE 2 More information may be found in ISO/IEC 30108-1.

This Technical Report defines a framework to address methods and approaches for remote and unsupervised enrolment, together with secure storage and transmission of biometric and supporting biographic data, covering a variety of both online connected and offline modes.

This Technical Report identifies the functional elements and components of a generic mobile biometric system and the distinct characteristics of each component. It provides guidance related to a generic mobile architecture with reference to supporting standards.

The context recognizes a) the user as being mobile and b) operation across a variety of platforms, particularly mobile devices but also including tablet, laptop and other personal computing devices. The key to defining this context is whether the user's environment is physically controlled by the organization to which the user seeks access.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37[1)], *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

1) For a freely available copy of ISO/IEC 2382-37:2012, see: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

3.1
mobile device
small, compact, handheld, lightweight 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 ICT devices, smartphones, USB gadgets.

3.2
personalization
ability to configure for a device to react in particular way for a specific individual

4 Abbreviated terms

BI Biometric interface

GPS Global Positioning System

GUI Graphical user interface

LAC Logical access control

NFC Near field communication

OS Operating system

OTG On-the-go – the USB connector of a smartphone

SE Secure element

TEE Trusted execution environment

USB Universal Serial Bus

5 The use of biometrics in mobile devices

5.1 Taxonomy of usage of biometrics in mobile devices

5.1.1 General

The context in which mobile devices can be used may be categorized, at a high-level, into four generic Use Cases. In all cases, usability and human factors should be considered and integrated into the development process of an application with use of biometric capability.

5.1.2 Generic considerations for all use cases

It is important to take account of the level of assurance required by providers and users of services in a mobile environment. These will depend on the nature of the service and environmental factors such as location, degree of remote control (if any), time, cryptographic and other security protection processes. Because the analysis of the security and assurance level is out of the scope of this Technical Report, the following clauses simply refer to high, medium and low levels of assurance. More detailed information on this aspect can be found in ISO/IEC 29115.

When implementing biometric services in mobile devices, it is important to note that irrespective of the biometric which is used or the application which uses it, the following functions should be considered:

a) capture of a biometric sample;

b) storage of a biometric reference (in some cases, this may be remote from the mobile device);

c) processing of biometric samples;

d) comparison of a biometric sample with a biometric reference (which may be remote from the device).

These general functionalities require some basic functions including:

a) capturing one or more biometric sample(s) from a sequence of samples (i.e. a facial image from a live view of a face);

b) establishing the best sample(s) based on some quality metric;

c) providing feedback to donor/subject for presentation of biometric (e.g. oval shape to position face);

d) providing a quality metric for sample capture;

e) providing feedback for failure to capture/failure to enrol;

f) providing information on what sensors are available on device (e.g. camera, multi-touch screen, finger scanner, GPS, accelerometer, etc.) together with any relevant technical details (e.g. touch screen resolution, number of multi-touches, camera resolution, etc.);

g) providing information on what biometric modalities have been captured as references;

h) comparison algorithms for each modality 1:1 and/or 1:few;

i) pass comparison score or pass fail result.

The application itself could handle some further biometric functions and fundamental identity management functions, such as:

a) ability to capture a new identity, delete or update an identity;

b) ability to handle exceptions;

c) processing of biometric samples.

These functions could form part of the OS framework. Consideration needs to be given to what elements may be resident on the device and what data may be processed remotely [e.g. via a web service, REST (Representable State Transfer), HTTP GET (Hypertext Transfer Protocol Group Encrypted Transfer), XML-RPC (Extensible Markup Language - Remote Procedure Call), etc.]. Different approaches may be taken in different circumstances, even for the same application. The device may be connected or not connected. At the platform level the user should see consistency in their interface.

Biometric comparison may be performed in the device or passed off to a remote server, depending on the use case and level of trust required.

A key aspect of mobile applications is the uncontrolled nature of the environment. The environment is one which is not controlled by the service the person is trying to access, so level of trust will be an important factor. Also, the environment could be different for each access occasion and vary over time.

In addition, it may be beneficial to use remote processing at a variety of system component interfaces. This would not only improve interoperability but allow biometric capabilities into systems that might not otherwise have them available. For example, an acquisition service such as WS-Biometric Devices (Web Services-Biometric Devices) would allow a mobile device without a built-in fingerprint scanner to acquire fingerprints from such an enabled scanner. A standard web service such as BIAS (Biometric Identity Assurance Service) may do the same for enrolment or recognition; for example, in cases where the data or comparison capabilities are not available locally. [Further information may be found in NIST/SP 500-288].

In any of the cases, certain general considerations should be addressed.

a) A decision should be taken on how the enrolment is performed, either in a supervised manner (external validation of the sample/s provided by some means) or in an unsupervised way (the user self-assesses the enrolment, with or without some quality check features on standards).

   In the case of unsupervised enrolment, it is recommended that the enrolment system automatically checks the quality of the samples provided (e.g. by following the relevant part of ISO/IEC 29794) and, when several samples are provided, the completeness of the union of all samples.

b) In order to protect the personal data of the device user it is recommended that both, the generation, and storage of the biometric probes and references, are protected so that there is no external access to these (e.g. from a third party application).

c) Although typically the device is to be operated by a single user, the possibility of more than one person using the device should be analysed with respect to the impacts of this on the device and assurance levels.

d) The computational power of a mobile device is expected to be less than that of a desktop computer or server. Therefore, analysis of the mobile device's biometric processing performance, given the resources available to the device, is recommended. Analysis should also be conducted on the performance of any sensor or biometric capture component built into the mobile unit, where the features of a built in capture component are comparably less than the feature set of an equivalent, specialist, stand-alone capture device.

e) Biometric services may be provided by the OS or by a third party application. In either case, the biometric services should run within a "sandbox" to limit the possibility of the biometric services running malicious code or accessing configuration data which affects the service's behaviour (e.g. decision thresholds).

5.1.3 Access to the device

This is a service offered locally at the device without the need of using on-line services. Typically, the decision is performed at the device itself, and a positive outcome will unlock the device and allow the user to access the rest of the services and applications installed in the device or offered remotely.

EXAMPLE Examples include using a personal biometric instead of a password, PIN or graphical pattern to unlock the device when it is turned on, or after a period of inactivity.

This service provides a minimum level of assurance to the device and the data and applications included. Applications and particular data access may require further authentications, which will raise the level of assurance. As the user of the device may want to access low assurance services (e.g. reading the news on a public newspaper), the mechanism of unlocking the devices should address convenience more than security, and, therefore, the level of assurance for this kind of use should be considered as low. The organization providing the device may consider raising such assurance level as to gain a more rigid control on the use of the device.

For user convenience in low security scenarios, after a fixed number of failed attempts, the device could offer an alternative modality or method (e.g. a password, PIN or graphical pattern could be offered as an alternative unlocking means).

5.1.4 Access to the local applications, services and/or data

This is a service offered locally at the device without the need of using on-line services. Typically, the decision is performed at the device itself, and requested by an application in order to allow continuing use of the application, or access to certain services, or control of the access to particular protected data. This should only be executed with the device unlocked and only by the application accessible at the main screen, to avoid unauthorized access by third-party applications or services.

EXAMPLE Examples include accessing a protected folder in the internal memory of the device, through a particular file explorer application.

The level of assurance required in this case depends on the application trying to authenticate the user, and the step to be accessed. Therefore, the level of assurance may change from one application to another. This means that thresholds (e.g. quality or comparison thresholds) may have different values depending on the assurance level demanded. In order to avoid misuse by third-party applications, consideration should be given to restricting the values of the thresholds so that they do not block the system nor pass everybody. The absolute miss threshold should never overlap the absolute hit threshold.

NOTE It is possible that the biometric service manufacturer may not be willing to provide different assurance levels, having fixed thresholds for its operation.

5.1.5 Access to the communications channel

This is an on-line mode of operation analogous to the situation of the previous case, but where the service or data to be accessed is located in a remote system. In this case the device is attempting to go on-line and open a communications channel to authenticate itself digitally to, and register on, that channel before being granted access. Instead, or in addition, biometric recognition may be used to authenticate the device user to the communications channel.

EXAMPLE Examples include verifying that a particular user is entitled to use a particular communications channel by the operator/owner of that channel, amongst other things for automatically implementing billing, credit and access policy.

Possible variations include:

a) local biometric authentication is used via some version of the mechanism described above, to release an authentication token that the communication channel trusts,

b) a biometric token is produced locally which is authenticated remotely by the system controlling access to the communications channel,

c) a biometric sample is sent to the remote system controlling access to the communications channel for processing and authenticated remotely against its enrolled user database,

d) federated systems where parts of data from more than one trusted source are combined.

When developing this kind of use case, the same considerations as in 5.1.3 should be taken into account, and, additionally, the following:

— identification mode or verification mode - processes may or may not be required to include an identity claim, e.g. device identifier such as IMEI (International Mobile Station Equipment Identity) number, or personal identifier via data stored on the device;

— validity duration of the authentication for the communications channel.

5.1.6 Verification/authentication of, or to, a remote resource or point of transaction

This is an on-line mode which may share the functional qualities of the processes described in 5.1.4, but where the owner/controller of the remote asset regards as insufficient or irrelevant the fact that the communications channel has already been authenticated.

EXAMPLE Examples may include situations where the communications channel has not been biometrically authenticated, and where the access policy and trust levels required are different from those of the communications channel provider. This might typically exist where a communications channel provides the carrier for a VPN (Virtual Private Network) service.

Consideration should be given to the security level achieved by the communication channel which may be reduced over time, therefore the biometric information exchanged, if any, should be additionally protected over the communication protocol.

5.2 Generic challenges in the integration of biometrics in mobile devices

5.2.1 Computational power

In the past, the lack of computational power of portable devices was one of the reasons for not considering viable the integration of several biometric modalities. But nowadays, after the spread of the new generation of 32-bit low power consumption microprocessors, this challenge is no longer such. In particular, if we consider that the computation needs will happen or be required when processing the biometric information inside the devices, it will only occur when using a one to one comparison (i.e. sample vs. biometric reference stored in the device), or as much, one to few comparisons, if there are several biometric references enrolled in the device. One to many comparisons can be run directly on a mobile device, but are more likely to be run on a central server, using a biometric sample acquired through the mobile device.

Sample acquisition and feature extraction may take considerably more time than comparison, especially in a 1:1 scenario. Also, for some modalities, implementations might code and compare features from every available frame so consideration should be given to processing extraction and comparison in real time.

There have been successful implementations of biometric modalities in mobile devices with examples being: fingerprint,[1] iris,[2] face,[3] hand,[4] voice,[5] and signature.[6] While processing does take longer due to limited processing power, in all cases, there has been no increase in reported error rates when compared to implementations on desktop computers. The provider should validate that the error rate has not changed.

5.2.2 Data protection and privacy

Currently, a mobile device carries a huge amount of personal data (i.e. data from the user, such as photographs, contacts, messages or even financial information), and/or confidential or reserved information from the professional life of the device owner (i.e. professional contacts, e-mails, documents, etc.). The access to all that information should be protected in a way that only the authorized person is able to access it. Therefore, authentication mechanisms should be used. A third-party may observe PIN code or gestural pattern entry, as mobile devices are frequently used in public places. The use of tokens have not been so widely implemented in mobile devices, as interfacing with the token will be accompanied by a set of usability constraints, due to the need of a connection slot for such token (i.e. a smartcard reader connected by OTG or Bluetooth). In addition, such token might be lost, stolen, or even copied.

Biometrics can be used to ease such a process, as long as the device is equipped with a biometric capture device (i.e. sensor). The user's biometric reference is also a piece of personal data that has to be protected from a non-authorized access. The direct access to the biometric reference may facilitate an attacker to impersonate the user of the mobile device, either in such a device, or in any other authentication process that may use that same biometric characteristic.

The reading or copying of credentials should be denied. Also, there should not be any possibility of overriding the authentication process. It is then when the traditional vulnerabilities of IT solutions are shown. As most of mobile devices are general purpose platforms, with the possibility of downloading any third-party application, it is feasible to get Trojan horses that may implement man-in-the-middle attacks, to manipulate data or the authentication process.

In addition, analogously to the case of copying of the user's PIN code or gestural pattern, biometrics may be "copied" and re-used by an attacker. Biometric data, in most cases, is publicly available (e.g. latent fingerprints, face photographs, iris photograph at a distance, etc.). Therefore, an attacker could obtain the raw information from the user and create artificial samples from it, trying to gain access to the system. This is usually known as presentation attack, or spoofing, requesting the need to include presentation attack detection mechanisms during the biometric acquisition process. More information on presentation attack detection may be found in ISO/IEC 30107.[7] The target of those mechanisms is to detect, and therefore deny, the presentation of samples that may be subject to be considered as artificial. In mobile devices, biometrics are only intended as being an authentication mechanism, not identification. Therefore, attacks such as obscuration (i.e. avoiding being identified) are out of the scope.

