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/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **2**
5 The use of biometrics in mobile devices ... **2**
5.1 Taxonomy of usage of biometrics in mobile devices ... 2
5.1.1 General ... 2
5.1.2 Generic considerations for all use cases ... 2
5.1.3 Access to the device ... 4
5.1.4 Access to the local applications, services and/or data ... 4
5.1.5 Access to the communications channel ... 5
5.1.6 Verification/authentication of, or to, a remote resource or point of transaction ... 5
5.2 Generic challenges in the integration of biometrics in mobile devices ... 6
5.2.1 Computational power ... 6
5.2.2 Data protection and privacy ... 6
5.2.3 Biometric sample capture ... 8
5.2.4 Sample authentication process ... 9
5.2.5 Usability ... 10
5.2.6 Solution testing ... 12
5.2.7 Challenges common to other scenarios and platforms ... 12
6 Biometrics services within the OS of the mobile device ... **13**
7 Biometric services at the application level in a mobile device ... **15**
8 Biometric application development [using the biometric engine(s) provided] ... **16**
9 Functional and operational guidance ... **20**
9.1 General guidance ... 20
9.1.1 Guidance on functional architecture ... 20
9.1.2 Guidance on environmental conditions and constraints ... 20
9.2 Guidance for enrolment ... 20
9.2.1 General guidance for enrolment ... 20
9.2.2 Supervised enrolment ... 21
9.2.3 Unsupervised enrolment ... 21
9.3 Guidance for authentication ... 22
9.3.1 Remote unsupervised authentication ... 22
9.3.2 Local unsupervised authentication ... 23
10 Use of multi-factor authentication ... **23**
10.1 Fusion and scores for multi-biometrics ... 23
10.2 Combining biometric and non-biometric authentication techniques for greater security and/or usability ... 24
11 Biometric modality specific guidance ... **24**
Bibliography ... **27**

© ISO/IEC 2016 – All rights reserved

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*.

© ISO/IEC 2016 – All rights reserved

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

© ISO/IEC 2016 – All rights reserved

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.

© ISO/IEC 2016 – All rights reserved

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.

© ISO/IEC 2016 – All rights reserved

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);

© ISO/IEC 2016 – All rights reserved