
**Information technology — Guidance
for specifying performance
requirements to meet security and
usability needs in applications using
biometrics**

*Technologies de l'information — Directives spécifiant les exigences
de performance afin d'atteindre la sécurité et les besoins d'utilisation
dans les applications biométriques*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	3
5 Authentication factors	3
5.1 Overview.....	3
5.2 Security and usability of authentication mechanisms.....	4
5.3 Knowledge-based authentication (PIN, passwords).....	5
5.3.1 General description with examples.....	5
5.3.2 Security considerations.....	6
5.3.3 Usability considerations.....	7
5.4 Possession based authentication (tokens, cards).....	7
5.4.1 General description with examples.....	7
5.4.2 Security considerations.....	8
5.4.3 Usability considerations.....	9
5.5 Personal characteristic based authentication (biometrics).....	9
5.5.1 General description with examples.....	9
5.5.2 Security considerations.....	11
5.5.3 Usability considerations.....	12
5.6 Multi-factor authentication.....	12
5.6.1 General.....	12
5.6.2 Example: token and PIN.....	13
5.6.3 Implementation options.....	13
5.6.4 Performance requirements for multi-factor authentication.....	14
5.7 Comparing security performance of authentication mechanisms.....	14
5.8 Summary comparison of authentication factors.....	15
6 Determining biometric authentication security requirements	15
6.1 General.....	15
6.2 Business requirements.....	15
6.3 Security-enhancing aspects.....	16
6.4 Suitable target figures for false acceptance rates.....	16
6.5 Other considerations in authentication security.....	16
6.6 Limits of authentication assurance.....	16
7 Determining biometric authentication usability requirements	17
7.1 General.....	17
7.2 Accessibility considerations.....	17
7.3 Throughput.....	17
7.4 Authentication failure rate for authorized users.....	18
7.5 Ease of use at point of authentication.....	19
7.6 Ease of use for enrolment.....	19
7.7 Other aspects of usability.....	19
8 Additional considerations in defining biometric security and usability requirements	19
8.1 Organization of requirements.....	19
8.2 Verification and identification modes of operation.....	20
8.3 Stages of authentication.....	20
8.4 Authentication assurance and standards.....	21
8.5 Application-specific performance considerations.....	21
8.5.1 Performance for business functionality.....	21
8.5.2 Performance for identity proofing and enrolment.....	22

8.5.3	Performance for identity verification	23
8.6	Additional security related requirements	23
8.7	Exception handling	24
8.8	Multi-factor authentication	24
8.8.1	General	24
8.8.2	Improved discrimination	24
8.8.3	Improvements in accessibility	25
8.8.4	Improvements in usability	25
8.8.5	Improvements in overall security	25
8.9	Dealing with security and usability shortfalls	25
8.10	Hypothetical example of quantitative performance requirements	26
9	Use cases	27
9.1	General	27
9.2	Time and attendance	27
9.3	Physical access control	27
9.4	Computer sign-on	28
9.5	Remote authentication	29
Annex A (informative) Risk assessment		31
Bibliography		40

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

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

Introduction

This Technical Report is aimed at helping readers to make informed decisions about the specification of performance requirements for authentication systems using biometric recognition in order to achieve desired levels of security and usability for the authentication process. Guidance extends to the use of biometric recognition with and without other authentication factors such as passwords and physical tokens. This Technical Report describes security and usability trade-offs in biometric recognition relative to those of other authentication mechanisms and provides advice on how to balance conflicting security and usability parameters in the context of real applications. In addition to a consideration of technical performance parameters such as biometric error rates and password strength, this Technical Report also addresses technical, human and procedural vulnerabilities associated with the various types of human authentication. Vulnerabilities when exploited can lead to an undermining of the integrity of the authentication result. These need to be considered as part of the risk management process which would seek to avoid risk or implement strategies to reduce risk to an acceptable level. This Technical Report builds on existing relevant standards and guidelines including those related to e-authentication and risk management.

Although some work has been done on examining the links between performance and security for biometric recognition, there currently exists no accepted rationale for comparing the security and usability of biometric recognition with that of passwords and other mechanisms.

It is useful to be able to compare biometric recognition as an authentication factor with other factors such as passwords and tokens. The latter have a wide existing deployment base and a well-established basis for setting security and usability performance parameters. However, comparisons between authentication factors are difficult because the strengths and weaknesses of the factors lie in different areas. In combination, the strengths of one factor can be used to counter the weaknesses of another. These considerations make the comparisons multi-dimensional and complex. Passwords are usually specified in terms of length and randomness in order to satisfy authentication security requirements. [10] However, it is well known that long and random passwords are difficult to remember and to enter and this is a usability problem. The historic understanding of password authentication and the trade-offs between security and usability provides a good reference against which to assess biometric recognition authentication performance.

As well as addressing the use of biometrics as a replacement for passwords or tokens, this Technical Report also considers the use of multiple factors (e.g. biometrics plus password) for authentication. This introduces another aspect of the trade-off decision, that of how to assess the performance requirements of the individual authentication factors when used in combination in order to meet an overall security and usability requirement. This Technical Report addresses this issue but the complexity of the subject limits the specificity of the advice that can be given.

This Technical Report provides guidance on performance considerations where biometric recognition is to be used for authentication to replace or augment the use of passwords or tokens. It also provides guidance for the interpretation of security and usability performance information in the application domain of interest so that suitable levels of security and usability can be achieved for single and multi-factor authentication.

Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics

1 Scope

This Technical Report provides guidance on specifying performance requirements for authentication using biometric recognition in order to achieve desired levels of security and usability for the authentication mechanism.

Guidance addresses issues such as the following:

- the biometric performance metrics that impact security and usability;
- comparing and quantifying the security and usability of biometrics and other authentication mechanisms, when used alone or in combination;
- how to combine performance of individual authentication elements in order to meet an overall security and usability requirement;
- the trade-off between security and usability in applications using biometric recognition;
- considerations in maintaining security and usability in systems incorporating biometrics.

The guidance is targeted towards applications that

- use biometrics for the authentication of individuals, and
- are of small to medium size (in terms of the number of enrolled individuals).

The guidance does not address the following:

- surveillance systems;
- systems whose primary aim is to detect and prevent attempts by individuals to create multiple enrolments under different identities;
- systems with a large and diverse population of enrolees, which can include people with special needs;
- other systems with a complex mix of functional, security and usability requirements.

Such large-scale applications are typically the domain of large organizations, and it is assumed that the developers of such systems will have access to appropriate biometric expertise able to provide guidance beyond the scope of this Technical Report.

This Technical Report does not address biometric modality and technology specific issues, nor does it provide quantitative biometric performance requirements that would satisfy a particular application.

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, *Information technology — Vocabulary*

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*