TECHNICAL REPORT

# ISO/IEC TR 29156

First edition
2015-11-15

# 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*

Reference number
ISO/IEC TR 29156:2015(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 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*

## 3 Terms and definitions

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

**3.1**
**accessibility**
usability of a product, service, environment or facility by people with the widest range of capabilities

[SOURCE: ISO 9241-171:2008, 3.2]

**3.2**
**authentication mechanism**
**synonym – authentication method**
process of identity authentication using one or more authentication factors

**3.3**
**authentication factor**
evidence to assert the identity of an individual

Note 1 to entry: Within this Technical Report, three categories of authentication factors are identified: possession based, knowledge based and personal characteristic based.

EXAMPLE ID card, smartcard, PIN, password, fingerprint, iris.

**3.4**
**biometric throughput**
number of users that a biometric system can process within a given time interval

[Source: Springer Encyclopaedia of Biometrics][11]

**3.5**
**effective entropy**
amount of randomness available within a particular authentication mechanism, taking into account implementation and procedural factors

**3.6**
**entropy**
measure of the amount of uncertainty that an attacker faces to determine the value of a secret

[Source: NIST SP800-63][10]

**3.7**
**exhaustion attack**
attack against the security of a system that attempts to determine the value of a parameter by testing all possible states of that parameter

**3.8**
**multi-factor authentication**
authentication based on more than one authentication factor

Note 1 to entry: In the context of this Technical Report, the multiple authentication factors encompass biometric + password, password + token, biometric + token and password + biometric + token. Combinations of biometrics such as iris + fingerprint are not included.

**3.9**
**raw entropy**
theoretical maximum amount of randomness available within a particular authentication mechanism

**3.10**
**system throughput**
number of users that an overall system can process within a given time interval (which is inclusive of the biometric throughput if biometrics are used)

**3.11**
**usability**
extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use

[SOURCE: ISO 9241-210:2010, 2.13]

Note 1 to entry: In the context of this Technical Report, usability is related to the ease of use of the authentication and the convenience it affords to the users (both subjects and operational staff). The following factors are addressed:

— throughput;

— authentication failure rate for authorized users;

— ease of use at point of authentication;

— ease of use for registering in the system;

— universality/accessibility.

## 4 Abbreviated terms

| | |
|---|---|
| DET | Detection error tradeoff |
| FAR | False accept rate |
| FMR | False match rate |
| FNMR | False non-match rate |
| FRR | False reject rate |
| FTA | Failure to acquire |
| FTE | Failure to enrol |
| LoA | Level of assurance |
| PIN | Personal identification number |
| ROC | Receiver operating characteristic |

## 5 Authentication factors

### 5.1 Overview

Traditionally, there are three classes of factors identified for achieving authentication of an individual (see, for example, ISO/IEC/TR 24714-1:2008, 5.1, NIST Special Publication 800-63:2006, 5.2[10], and Reference [12]):

— Knowledge based: Something you know, normally a password;

— Possession based: Something you have, normally a physical token;

— Personal characteristic based: Something you are, normally known as biometrics.

Although each of these factors can be used to achieve the goal of secure authentication, the way in which they operate and what they depend on is different. The first method relies on the secrecy of the password. The second method relies on the exclusivity and control of the physical token. The third method relies on the distinctiveness and persistence of an individual's biometric characteristics.

No authentication technology works perfectly at all times and under all circumstances. Each one has performance limitations and potential security and usability problems, and the optimal choice will depend on the application and its environment of use. In some cases, a combination of authentication factors will be an optimum solution, but in all cases, there will be a need for exception handling procedures to deal with authentication failures that will invariably occur in operational use.

Authentication using more than one factor (e.g. token plus PIN) is known as multi-factor authentication. In this context, different biometric modalities do not qualify as different factors and a biometric system using more than one modality (e.g. fingerprint plus face) is known as a multi-biometric system. These possibilities are not mutually exclusive; an authentication system could be both multi-factor and multi-biometric.

5.3, 5.4 and 5.5 give an overview of the authentication factors and describe the main performance parameters that control and limit their security and usability, which are the following:

— discrimination (related to the amount of information contained in an authentication factor, the number of states that it can occupy and hence its resistance to a direct attack);

— memory (the reliance of the method on human memory capability);

— discovery (the ease with which the method is vulnerable to guessing or spoofing, etc.);

— shareability (the degree to which the secret contained in the factor is readily shareable and thus potentially vulnerable to social attack);

— usage (how available, acceptable, and prevalent the technology is);

— reliability (the consistency with which the implementation performs);

— ergonomics (ease of use);

— manageability (administrative burdens incurred by use of the implementation including exception handling).

## 5.2 Security and usability of authentication mechanisms

When discussing the security of authentication, we are referring to the risk that an impostor could succeed in being authenticated thereby gaining access to the assets that should be protected by the authentication mechanism. Such security failures might occur for a number of reasons that include both technical and procedural failures. Security weaknesses of authentication mechanisms (and security measures in general) are usually divided into two categories:

a) Inherent limitations of the mechanism which are present even when it is implemented perfectly.

b) Failures of design, implementation and operation that allow the mechanism to be subverted or bypassed.

Authentication mechanisms that have a probabilistic outcome have inherent security limitations. Password and biometric recognition mechanisms are instances of this. Passwords can be discovered through chance guesses or exhaustion attacks without any knowledge of the implementation. These are known as direct attacks. The defence is to increase the password space in order to render the chance of a correct guess to a very low probability or make the amount of effort needed to conduct a successful exhaustion attack beyond that which is reasonably feasible. Biometric recognition has analogous limitations. An impostor could succeed in being authenticated if by chance their biometric characteristics are very similar to those of the one enrolee for whom the claim of identity is provided, a false match error. In both the password and biometric cases, an impostor can seek to exploit the inherent limitations through direct attack. It is possible to reduce the likelihood of successful exploitation to any defined low probability but in doing so the usability will normally suffer and may become unacceptable in operational use. In practice, a balance has usually to be struck between security and usability.

The resistance to direct attacks on the intrinsic limitations of the authentication mechanism is a measure of the strength of the mechanism and this strength is represented by appropriate performance parameters. For biometrics, the relevant performance parameter for strength is the false match rate. For passwords, it is the level of uncertainty given by the allowable choice of passwords. This is commonly expressed in terms of password entropy and this concept is covered in more detail in the following sections and in NIST Special Publication 800-63:2006, Annex A.[10].

The security weaknesses represented by b) are termed extrinsic vulnerabilities. These vulnerabilities occur as a result of imperfections in the design, implementation or operation of the mechanism. Attacks that exploit these vulnerabilities are indirect. They seek to subvert or bypass the authentication process and can involve technical, human and procedural factors, often a combination. Examples for password authentication could include a poorly implemented password system that allows the use of passwords selected in a non-random manner or includes an embedded “testers” password (technical) and passwords written on sticky notes (human/procedural). For biometrics, potential vulnerabilities include presentation attacks (spoofing) using artefacts and poorly designed biometric algorithms that display an exceptionally high false match rate for certain specific biometric samples. For tokens, potential vulnerabilities include lost control of the token, skimming of information from contactless chips, or cloning of smartcards or ID cards. Exploitation of technical vulnerabilities usually requires knowledge of the implementation of the mechanism and time and expertise to develop successful attack techniques.

Vulnerabilities need to be addressed as part of a system risk assessment and mitigation process and the findings incorporated in the system security policy and associated secure operating procedures.

Security and usability of authentication mechanisms is only one element of the wider security and usability picture that affect the overall system security and usability. These wider issues should be addressed by the system security policy and a corresponding usability policy. Detailed consideration of risk and usability assessment methodologies lies outside the scope of this Technical Report and the information provided in later sections is limited to general guidance supplemented by references to external documents and relevant standards.

## 5.3 Knowledge-based authentication (PIN, passwords)

### 5.3.1 General description with examples

Knowledge based authentication relies on a secret that should be known only to the subject of the authentication. This is commonly implemented in the form of a secret PIN or password. The security assurance of authentication by means of a knowledge based mechanism is related to the possibility that the user’s secret knowledge could become known by an impostor. The probability that an impostor might discover the password by trial and error attempts is dependent on the number of attempts that can be made and the size of the password space that needs to be explored. With more positions and variable characters, as well as fewer permitted retries, the probability of guessing a PIN or password decreases. It is technically straightforward to increase the available password space to render the discovery of passwords through exhaustive trial attempts beyond reasonable possibility but that approach often creates overwhelming usability problems for the subject due to the difficulty of memorizing the password and entering it correctly.

EXAMPLE 1 If passwords are limited to one character from the Roman alphabet, the entire password set can be exhaustively searched in 26 attempts. For a randomly chosen password, the average number of attempts to discover the password is 13.

EXAMPLE 2 If passwords are 10 characters long, are randomly chosen and can include both upper and lower case letters, numbers and punctuation marks of a standard keyboard (94 symbols), an exhaustive search would need up to $94^{10}$ ($\sim 5{,}4 \times 10^{19}$) attempts to discover a password via an exhaustion attack, and half that number on average.

### 5.3.2 Security considerations

#### 5.3.2.1 Performance parameters for security

The core security performance parameter for a knowledge based authentication method is a measure of the effort required to determine the secret by means of an exhaustion attack. It can be expressed in terms of the uncertainty of success associated with a single guess or trial as part of an exhaustion attack. This approach is useful because it allows the analysis of passwords to make use of the “entropy” based technique used for calculation of uncertainty in communication theory problems. Further information on entropy and how the entropy concept can be applied to password analysis can be found in Reference [10]. Entropy can be the metric of password strength.

#### 5.3.2.2 Security vulnerabilities

##### 5.3.2.2.1 General

A password provides no assurance that the person presenting the password is who they claim to be. This is an inherent limitation when using passwords to authenticate users.

A weakness of any knowledge based authentication mechanism is that the secrecy of the information can be compromised. Voluntary compromise can occur by sharing a user’s User-ID, PIN and/or password with another individual. Involuntary compromise can occur by discovery of a written record of the knowledge (e.g. list of passwords) or by covertly observing the user’s information entry (e.g. “shoulder surfing”).

Password attacks can be broadly divided into three key categories as described in the following subclauses.

##### 5.3.2.2.2 Manual entry of trial passwords

Manual attempts by repeated entry of trial passwords via the normal system password input procedure is a form of attack that requires opportunity and patience but no expertise. It can be made more difficult by the imposition of operating procedures that limit the number of consecutive failed password attempts to a small number before a lockout occurs[1)]. The attacker is then forced to spread the attack across multiple sessions which will be much more time consuming and increases the chance of being caught. Manual attacks are made easier if the attacker can predict likely passwords from knowledge about the subject being targeted. Generally speaking though, manual attacks can be thwarted by password policies that enforce reasonable entropy requirements for password choice and implement a multiple failed attempt lockout policy (but see 5.3.2.2.3).

##### 5.3.2.2.3 Discovery of the password by a failure of security external to the system

Passwords can be obtained or discovered through external security failures such as shoulder surfing or when passwords are written on a sticky note attached to a terminal. This should be regarded as an extrinsic security weakness or vulnerability of password systems. Paradoxically, attempts to improve password security by imposing rules that increase password entropy may have a counterproductive effect on security, because such passwords are usually more difficult to remember and are therefore more likely to be written down by users and left somewhere “handy”. Password policy should be considered as part of the overall system security policy. It is not addressed further in this Technical Report.

##### 5.3.2.2.4 Offline mechanized attacks

The threat of mechanized attacks on password files is the main reason for requiring high entropy for passwords. Passwords are not stored in “clear” in the password file; that would be far too insecure. Instead, the password is transformed by a cryptographically strong hashing algorithm into a number or password “hash” which is stored in the file. In this way, if the file contents are discovered, the hash

[1)] This implies some sort of computer controlled password system. Mechanical combination locks, etc. do not usually have the capability of limiting the number of attempts in a session.

values cannot be used directly as passwords. When a password is entered by a user, it is transformed in the same way as for the original password setting process and the hash value thus produced is compared directly with the hash value corresponding to that user stored in the password file. Thus, passwords are not compared, only their hash values. If the hash values agree, then the user is authenticated.

The assumption for a mechanized attack is that the attacker has somehow acquired a copy of the system password file and has access to the algorithm that has been used to “hash” the passwords in the file. The attack comprises the generation of trial passwords based on dictionary words, combinations and simple transformations, usually ordered by some knowledge of prior probability. Each trial password is transformed to the corresponding hash value and the trial hash compared against one or more hash values in the copied system password file. This process is repeated for all the trial passwords until a “hit” is found or the attack terminates in failure. Using modern computers (sometimes networks of computers) “hits” can occur in often surprisingly short timescales because of the non-random choice by users of “easy” passwords.

The principal requirements for the password hashing algorithm are to ensure that the hash values it produces are as nearly as possible randomly distributed numbers across the total available hash number space; that the same password will always be transformed to the same hash value; and that hash values cannot be reverse engineered to discover the original passwords. An additional practical requirement is to ensure that the hash number space is much greater than the password space (i.e. the entropy of the hashes ≫ entropy of the passwords). This ensures a very low probability of password collision; two different passwords transforming to the same hash value.

#### 5.3.2.2.5 Other methods of attack

A number of other attack methods are available such as the use of keyloggers, Trojans, phishing attacks, etc. These are beyond the scope of this Technical Report and are not discussed further.

### 5.3.3 Usability considerations

#### 5.3.3.1 Performance parameters for usability

The performance parameters for usability for a knowledge based authentication factor may be dependent on the specific application, and could include the following:

- proportion of knowledge entry attempts correctly entered/accepted;
- number of attempts on average to successfully enter knowledge value;
- frequency of need for help with knowledge information reminder or refresh (help desk calls);
- frequency of lockout;
- user satisfaction survey results when questioned about knowledge based authentication methods.

#### 5.3.3.2 Usability problems

Knowledge-based authentication factors may also lead to problems such as

- multiple sign-on requirements for differing password strength policies, and
- frequent forced changes in passwords which lead to recording or forgetting current values.

## 5.4 Possession based authentication (tokens, cards)

### 5.4.1 General description with examples

The possession in “possession based authentication” is usually a plastic card or token. The user is expected to keep this token under his/her sole physical control. Tokens can contain two different types