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 of authentication information: features used to automatically verify the authenticity of the token, and information used to validate the authorized user of the token. Examples range from magnetic stripes to tamper-resistant microcontroller chips that possess contact-based or contactless communication interfaces and are able to store private or shared secret keys and to execute cryptographic algorithms on behalf of the user. To avoid misuse when a card or token is lost, stolen, or left lying around, cards and tokens may be accompanied by additional user authentication by means of PINs or passwords or by means of biometric recognition mechanisms. The use of tokens within a multi-factor solution of this type is described in more detail in 5.6.

5.4.2 Security considerations

5.4.2.1 Performance parameters for security

Tokens can vary considerably in sophistication and security. In the absence of any binding between the token and the user, the mere possession of the token is not normally considered to provide sufficient assurance of the authentication of the user.

The security parameters for smart token implementations are determined by the strength of the cryptographic mechanisms employed and by the physical construction that provides tamper resistance to prevent the creation of fake tokens. With modern technology this strength can usually be considered strong. However, this can only provide assurance of the authenticity of the token, not of the user. The binding of a token to a user normally depends on a PIN which is the weakest link in the overall authentication process.

5.4.2.2 Technical security vulnerabilities

Current smart tokens are physically and cryptographically secure. Highly sophisticated technical attacks have been demonstrated by researchers under laboratory conditions including gaining physical access to the chip and connecting to internal circuitry to read stored data and probe for internal signals and to monitor patterns of chip power consumption to provide insight into the operation of the cryptographic algorithms. The main aim of the investigations is to discover if secret information stored on the card such as cryptographic keys can be acquired and used to fabricate a forged card. However, such attacks are extremely difficult to mount and there is little current evidence of any significant attacks of this kind on commercial smartcard based authentication applications such as credit/debit cards, etc. In practice, there are far easier ways to attack smartcard based authentication systems than by attempting to exploit technical vulnerabilities of the card.

5.4.2.3 Human/procedural security vulnerabilities

Users sometimes put convenience ahead of security and will lend their token to another person to conduct transactions on their behalf. This occurs in domestic and working environments and such practices have a serious impact on the authentication assurance. How important this is depends on the application and the context. The issue is one of accountability for transactions and the consequences of contentious or unaccountable transactions. For example, the loan of a card to a family member to obtain cash is not a serious issue most of the time and the responsibility and accountability remain within the family. In a working environment, the sharing of tokens among staff members can have serious consequences in the event of a problem leading to the need to establish accountability for actions. Authentication using biometric recognition is not subject to this sharing vulnerability.

Human/procedural security vulnerabilities include bypass attacks. An example of this is where a technical security measure is optional such as with a chip and PIN card where alternative authentication methods are allowed in cases where the chip and PIN infrastructure is not available. The alternative may be much less secure, defaulting to that of a magnetic stripe card, i.e. a signature or knowledge of the security number or nothing.

5.4.3 Usability considerations

5.4.3.1 Performance parameters for usability

Generally, tokens are easy to use. They can combine the desirable properties of good usability and high technical security without trade-offs, unlike other forms of authentication such as passwords and biometrics. Some users with physical or cognitive disabilities may have usability problems but these are more likely to be associated with any associated PIN rather than the token itself. However, the authentication assurance is assurance of the authenticity of the token and not the user. A token-specific usability parameter is the time taken for reading and checking the token from placing the token on the reader until removing the token.

5.4.3.2 Technical usability problems

The only technical usability problems are likely to be with technical failures of tokens and readers. Setting aside intentional damage, tokens are usually quite robust. They can be damaged by accidental maltreatment, e.g. excessive temperature, microwave radiation, repeated physical flexing. The effect of technical failures is usually to precipitate procedural usability problems.

5.4.3.3 Human/procedural usability problems

In order to use a token based system effectively, the user should understand how to interact with the system. In general, the usability of such systems is enhanced by the provision of good user guidance, unambiguous signage and so on.

If a token is damaged, the failure will probably be detected only on next use, which may create an immediate problem for the user, particularly if no alternative is readily available. Once damaged, repeated attempts to use the token are unlikely to be successful and restitution of service will be delayed until a new token can be made and delivered to the user. In many cases, the delay will be measured in days or even weeks which could create a serious usability problem. In applications where such delays are unacceptable, alternative measures will need to be available. This could be in the form of a temporary token that can be supplied quickly or a non-token based exception handling procedure. Both of these may have adverse effects on the security of the authentication process.

5.5 Personal characteristic based authentication (biometrics)

5.5.1 General description with examples

Biometric recognition is the automated recognition of individuals based on their physical and behavioural characteristics. Commonly used physical characteristics include finger ridge patterns (usually called fingerprints for simplicity), face features, hand geometry, hand and finger vein patterns and iris patterns. Behavioural characteristics include signature dynamics (the way in which individuals write their signatures or other personally identifying information) and keyboard dynamics (the way in which individuals type words or phrases on a keyboard). Voice is an example of a biometric characteristic that combines physical and behavioural elements.

Because biometric characteristics are intrinsically linked to the individual, they can provide a higher level of assurance than other factors that an authentication is genuinely that of the individual.

Authentication using biometric recognition can also offer benefits in usability because there are no difficult passwords to memorize and no tokens to remember to carry.

Biometric recognition systems acquire biometric samples from biometric characteristics, extract features from the samples in a form suitable for storage and comparison and compare the converted data with reference data previously acquired and stored during enrolment. If the sample and reference are sufficiently similar, a match is declared; if not, a non-match results. Because there are variable factors both with the biometric characteristic itself and with the acquisition process, exact matching is not expected to occur. This has two ramifications, firstly, that a decision threshold has to be employed to decide whether the sample and reference are a true match or not, and secondly, that the decision is subject to error.

Decision errors are of two types: a false match where a match is declared for a sample and reference that were not acquired from the same biometric characteristic of an individual and a false non-match where a non-match is declared for a sample and reference that do come from the same biometric characteristic of the individual. These are the two principal types of error that affect security and usability of biometric systems.

There are two other relevant error conditions. "Failure to enrol" errors occur when individuals are unable to successfully complete the enrolment process, thus preventing them from being subsequently authenticated biometrically. Failures to enrol can have a serious effect on accessibility and usability of a biometric system. They can also undermine security if alternate authentication measures provided for those that are not enrolled biometrically are less secure than those for normal users.

Finally, an acquisition error can occur which prevents a biometric sample being acquired from an individual. This is termed a "failure to acquire". While isolated acquisition failures may be overcome with a subsequent successful acquisition, persistent failures to acquire cause rejections. Failures to acquire, together with false non-matches, determine the biometric system false reject rate.

The occurrence of these biometric errors means that the recognition outcome is not a certainty but a probability controlled by the likelihood of false matches and false non-matches. The errors are normally expressed statistically in terms of the average rate at which they occur across a large population of individuals and a large number of trials.

In summary, these are the following:

- Failure-to-enrol rate, FTE;
- Failure-to-acquire rate, FTA;
- False non-match rate, FNMR;
- False match rate, FMR;
- False reject rate, FRR;
- False accept rate, FAR.

The negotiation of the matching threshold and the resulting FARs and FRRs is a tool that biometric system designers and implementers can adjust to suit different needs and applications of the system. For instance, if the threshold is made to be more stringent, then the system will block more imposter users from being falsely accepted (higher security), but also will falsely reject a greater number of genuine users (reduced usability). Conversely, if the threshold is made to be less stringent, then a greater number of imposter users will be falsely accepted (lower security); but a smaller number of transactions by legitimate subjects will be rejected (increased usability).

For verification performance requirements specification, the distinction should first be made between single attempt and multiple attempt operations. Typical biometric applications allow for retries in the event of a failure to match on one attempt, and if so, the number of allowable attempts should be stated. Then, a transaction is defined as one or more attempts (up to the stated limit).

- For specifying the Security aspect of matching, FMR is used for single attempts, and FAR is used for transactions.
- For specifying the Usability aspect of matching, FNMR is used for single attempts, and FRR is used for transactions.

These metrics are typically illustrated on an ROC or DET curve. An example of the latter is shown in Figure 1. Most biometric devices can operate at various points along these operating curves, and the choice of the matching threshold determines where on the curve. Figure 1 illustrates the performance of two different devices: device A (dotted curve) and device B (solid curve). In this illustration, device A has superior matching performance compared to B.

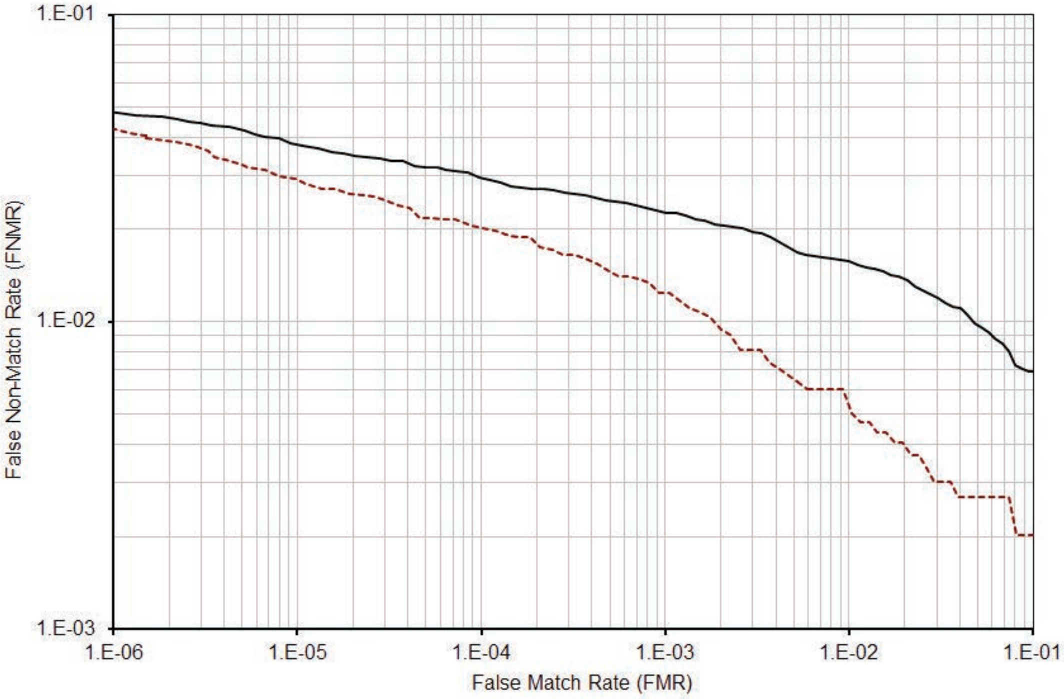


Figure 1 — Example DET Curves

Conventional metrics used to assess biometric performance (FAR, FRR, etc.) are measured with "zero-effort imposter attempts". Imposter attempts are defined as zero effort if the individual submits their own biometric feature as if they were attempting successful verification against their own template. The existence of some biometric system vulnerability to presentation attack or spoofing (e.g. using artefacts such as latex fingerprints) has been published and cannot be ignored. Metrics for assessing the performance of a biometric system to resist presentation attacks (at the biometric sensor) are the subject of other standards activities (see, for example, Reference [6]) and are not addressed here. The requirements definition process should consider conventional performance metrics, as well as spoof and other presentation attack mitigation metrics from the perspective of the application.

5.5.2 Security considerations

5.5.2.1 Performance parameters for security

The performance parameters for both security and usability are interrelated and are discussed in detail in 5.5.1 and Clause 8.

5.5.2.2 Technical/human/procedural security vulnerabilities

Even though biometrics can help alleviate the problems associated with the other methods of user authentication, there still are weak points in the system vulnerable to attack. Yet there are several new types of attacks possible in the biometrics domain. Many of these may not apply if biometrics is used as a supervised authentication tool. But in the remote, unattended environment, imposters may have the opportunity to make several attempts, or even physically violate the integrity of a remote client, before detection. This Technical Report identifies these vulnerable points and makes suggestions on how to take advantage of biometrics while alleviating vulnerabilities.

5.5.3 Usability considerations

5.5.3.1 Performance parameters for usability

The performance parameters for both security and usability are interrelated, and are discussed in detail in 5.5.1 and Clause 8.

5.5.3.2 Technical/human/procedural usability problems

Usability covers the less extreme end of the accessibility/usability spectrum; problems that adversely affect the efficient operation of a biometric system as a result of non-optimal interaction between the users and the system.

ISO 9241-11 defines usability as:

The 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.

The usability of a biometric system will be affected by its design and technology and the way it is implemented and operated in its working environment. Usability may be considered from different viewpoints, the viewpoint of the system and the viewpoint of the subject being the two principal ones. Authentication system usability is typically characterized by metrics such as cost, throughput rate and performance. From the subject viewpoint, usability will generally reflect the overall user satisfaction with the process, which will include ease of use, time taken and rate of success and also less tangible factors related to ergonomic design and environment. There are often common factors between good system and subject usability measures, for example, throughput and time taken, but they do not always track exactly because user satisfaction is dependent on a range of factors, time taken being only one. For example, the system throughput measure does not directly measure ease and convenience of use for the subject or whether the system is unpleasant to use because e.g. it involves a strong light shining in their eyes. Similarly, the error rate performance parameters of a biometric recognition system do not fully characterize the range of usability factors that affect the overall usability of the system.

The use of biometrics as an authentication factor can introduce its own form of usability problems, including the following:

- the modality chosen may not be accessible to the whole target population, leading to failures to enrol;
- samples may not be acquired due to technical factors (e.g. poor performing sensors) or human/procedural factors (e.g. non-conformant presentation) causing a failure to acquire;
- transaction duration may be longer than for other authentication factors;
- some samples that should match do not (false rejections);
- ergonomic design may not be suitable for some subset of the population.

NOTE Ergonomic issues also affect other authentication technologies but are particularly relevant to biometrics.

Some systems will have an operator or supervisor who is able, to some extent, to address such issues when they arise. This process can be greatly assisted for some modalities if the operator/supervisor is provided with an image of the biometric sample at an appropriate size and quality.

5.6 Multi-factor authentication

5.6.1 General

Multi-factor authentication involves the use of more than one of the previously discussed authentication factors in a single authentication mechanism, with the intent of strengthening the overall authentication assurance (higher security). Utilizing multiple independent factors will mitigate some of the first-order vulnerabilities for any given factor if used alone. Multi-factor authentication mechanisms will be more difficult to circumvent by an attacker. Conversely, multi-factor authentication mechanisms can be more difficult for the user to execute (reduced usability) and more complex to implement.

5.6.2 Example: token and PIN

Possession based authentication is often used as part of a two factor authentication process because the possession of the token alone is considered weak for authentication of the authorized user as it can readily come into the possession of an unauthorized person. For some applications, such as access to and charge for a public service like transportation, it is the authentication of the card rather than the holder that is important and the presence of the token is sufficient for the purpose. However, where authentication of the user is required there needs to be some means of linking the token to a specific authorized user. The commonly used approach to providing this “binding” is by means of a PIN which should be known only to the authorized user. The PIN is used to authenticate the user to the card or to the application that is using the card.

Modern chip based tokens (e.g. smartcards) embody substantial computing power and data storage which enables the use of advanced cryptographic techniques to provide strong authentication of the token itself to the application. With the use of a PIN to authenticate the user to the token (or to the application), the user authentication assurance is the assurance that the PIN provides supplemented by the fact of possession of the token. An impostor would need to acquire the token and to know the PIN or to determine it through a trial and error process. The feasibility of this will depend on the application. Many card/PIN based applications will only allow a small number of failed attempts at entering the correct PIN before timing out either for a period of time or until reactivated using a secure exception procedure.

The gain in assurance over that provided by a PIN alone is difficult to quantify. It will depend on the assumptions made, for example the proportion of tokens that are assumed to be in the hands of unauthorized users at any one time and the average window of opportunity for misuse before the loss or theft of a token is notified to the issuing authority and the token revoked. Clearly, tokens acquired by criminals are likely to be presented quickly in order to exploit the window of opportunity.

Most of the vulnerabilities of token/PIN based multi-factor authentication are the normal vulnerabilities associated with the PIN. PINs are generally short (4 digits is common) which have the merit of being more memorable than longer passwords, especially when used infrequently. Nevertheless, some people have difficulty remembering PINs, particularly when they have several different cards and PINs and in some cases they may write the PIN on the card. If the card should fall into the hands of an unauthorized user, exploitation is trivial if undertaken before the card has been revoked. A criminal may also acquire the PIN through observing the authorized user entering it (shoulder surfing) prior to stealing the card.

A substantial procedural vulnerability exists in cases where the use of token and PIN together is not mandatory. Where the national or local infrastructure does not support chip and PIN authentication, the levels of authentication assurance provided by the token is likely to be substantially reduced, essentially to that corresponding to possession alone or even simply knowledge of data appearing visually on the token. For compatibility with previous generations of magnetic stripe cards, some smartcards also embody a magnetic stripe for use with transactions when the chip and PIN infrastructure is not available. Telephone and online transactions usually accept smartcard payment without chip and PIN authentication. Additional online authentication assurance is sometimes provided through a separate online password authentication process via the card company’s IT system.

An unauthorized user will seek to exploit procedural vulnerabilities which are invariably easier to attack than technical vulnerabilities. In cases where the infrastructure does support chip and PIN authentication, an imposter may attempt to force a failure of the chip and PIN authentication process in order to exploit procedural vulnerabilities of the fall-back process. This can readily be done by damaging the contacts or the chip itself, physically or electrically.

5.6.3 Implementation options

It should be noted in discussing multi-factor authentication, that there are at least two methods of implementing this, serial (chained) or parallel (concurrent).

In the chained approach, one factor activates/enables a second factor which is what is presented to the verifier. This is depicted in Figure 2.

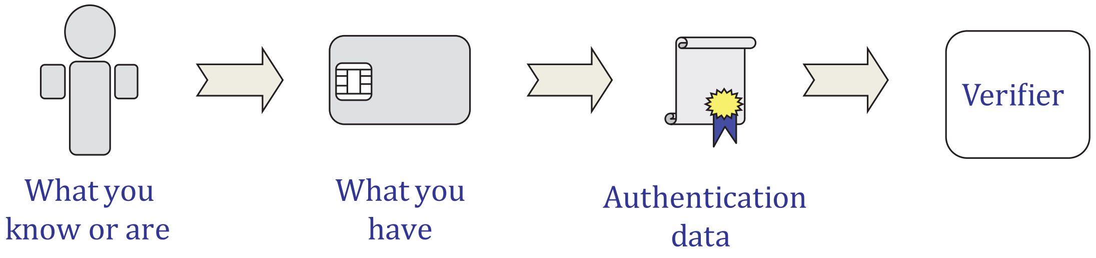


Figure 2 — Serial multi-factor authentication

In the concurrent approach, both factors are provided by the user and are independently verified at the verifier, as shown in Figure 3.

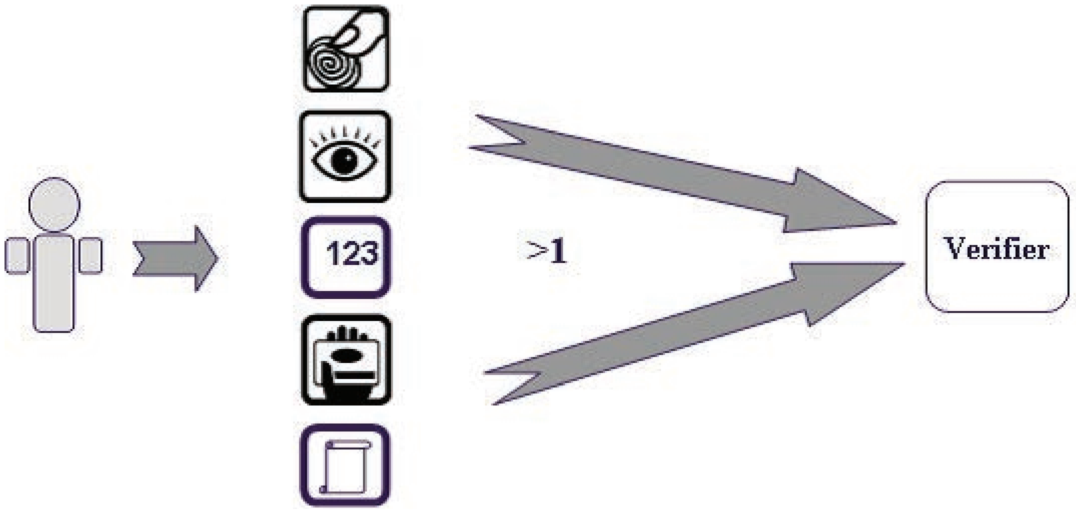


Figure 3 — Parallel multi-factor authentication

5.6.4 Performance requirements for multi-factor authentication

Depending on the implementation chosen, it might be possible to attack and surmount the factors individually. If this is the case, the security-relevant performance parameters for each factor will need to be more stringent than in the case where the factors are not separable.

5.7 Comparing security performance of authentication mechanisms

Reference [13] introduces the concepts of raw and effective entropy when determining relative strengths of function and its relationship to binding strength, which is the confidence that a person presenting an authentication credential is who they claim to be.

The strength of an authentication mechanism is determined by its strength in three component areas.

— Discrimination: the ability of a mechanism to distinguish between individuals. Lack of discrimination is the exploitation avenue most used for casual (low or zero-effort) attacks.

— Technical strength: the resistance of a mechanism to attacks such as exhaustion attacks which exploit the vulnerabilities of that mechanism, as well as indirect attacks against the supporting infrastructure (e.g. transmission paths, databases).

— Human or procedural strength: the ability of a mechanism to resist attacks based on social engineering, “easy” secrets, failure to guard secrets, and corrupt users/administrators. This element reduces effective entropy sometimes to zero.

Reference [13] also provides an example of such a comparison for passwords and biometrics.

5.8 Summary comparison of authentication factors

The prevailing techniques of user authentication involve the use of either user names with passwords or ID cards with PINs. Both of these two scenarios contain a secret, knowledge-based component which the user must enter into the authentication system. Passwords and PINs can be acquired by direct covert observation. In applications protected with a single-factor knowledge-based authentication mechanism, once an attacker acquires the user name and the password, they have total access to the user’s resources. In addition, there is no way to positively link the usage of the system or service to the actual user; that is, there is no protection against repudiation by the user name owner. For example, when a user name and password is shared with a colleague, there is no way for the system to know who the actual physical user is. A similar situation arises when a transaction involving a credit card number is conducted on the Internet. Even though the data is sent over the Internet using secure encryption methods, the systems are not capable of assuring that the transaction was initiated by the rightful owner of the credit card.

The level of security and usability associated with biometric recognition when used as an authentication mechanism varies based on the modality employed (e.g. fingerprint, face, voice, iris) and on the individual design and implementation of the technology. The use or addition of biometrics as an authentication factor can mitigate the fundamental weaknesses of physical tokens used alone (lost token vulnerability) or the compromise of secret knowledge, thereby providing a greater degree of assurance of the identity of the user. This Technical Report will not address modality and technology specific issues; rather, it will concentrate on intrinsic performance requirements to meet security and usability needs. With this information, prospective customers will be able to approach suppliers with a performance specification that will enable them to determine whether the modalities and technologies on offer are able to meet their requirements for security and usability.

6 Determining biometric authentication security requirements

6.1 General

This Technical Report addresses security considerations of the performance of authentication using biometric recognition in a system where authentication failures can cause breaches of the system security policy. For example, in physical access control systems there needs to be an assurance that only authorized persons are granted access. Likewise, in a time and attendance system, employees should not be able to clock in or clock out someone else.

6.2 Business requirements

The owner of a system using authentication mechanisms to improve the security of their system understands the problem from a business perspective. In that sense, the owner can be expected to provide definitive input into the “operational business requirements” development process. Starting with business requirements, a “top-down” approach should be used to think about these business requirements in terms of their enabling technical requirements. At this level, the choice of a specific authentication mechanism is only part of a broader view of the overall system-level technical requirement (such as detection of intrusion attempts, intrusion alarms and responses, operating environment, and mode of operation).

Business requirements for the application should drive the risk analysis which results in identifying and quantifying security and usability requirements. Some of these requirements may be determined externally (see Reference [10]). Examples of external requirements could be service level agreements with other organizations and applicable legislation restricting the collection and storage of personal biometric data.

6.3 Security-enhancing aspects

Assuming that biometrics are included as one of the authentication mechanisms, the next layer down in the requirement generation process is to focus attention on the security enhancing performance aspects of biometrics (note that the convenience, usability aspects are addressed in Clause 7, but relationships between security/usability should be acknowledged). At this point, the key consideration can include the following:

- permissible level of false acceptance;
- impact of failure to enrol (How secure is the intended secondary procedure? Is a secondary biometric needed?);
- resistance to/detection of active imposter attacks at the biometric sensor point of attack (spoofing, liveness, artefacts, etc.).

6.4 Suitable target figures for false acceptance rates

In terms of the protection offered by authentication mechanisms, for the common password case, the 4-digit PIN is widely accepted as a security measure offering a basic level of authentication assurance. 4-digit PINs are used fairly ubiquitously for authentication, sometimes alone, e.g. push button door entry locks, but often in association with a smartcard token for, for example, banking transactions, this being an example of two-factor authentication.

As a simple rule of thumb, it is suggested that for basic, medium and high levels of authentication assurance, rates of 1 % (1 in 100), 0,01 % (1 in 10^4) and 0,000 1% (1 in 10^6) can be considered as suitable target figures for false acceptance rates for biometric recognition. These figures are roughly commensurate with the increasing authentication assurance provided by longer and more complex passwords. Requiring a higher level of assurance (i.e. lower false acceptance rates) is likely to impact usability, either increasing the number of rejections or requiring greater effort or time on the part of the subject.

6.5 Other considerations in authentication security

However, these performance parameters only address one aspect of the overall authentication assurance, which is ultimately limited by vulnerabilities in the implementation and operation of the overall authentication process. For passwords, this includes “shoulder surfing”, poor choice of passwords and passwords written down in places accessible to impostors. For biometrics, other considerations include the following:

- presentation or spoofing attacks using artefacts;
- algorithms for which FAR varies substantially across users, such that certain individuals may have a much higher FAR than others.

While password vulnerabilities are mostly related to poor usage and management which are easy to understand (if not always to counter), biometric vulnerabilities tend to be technical in nature and are only likely to be exposed through a security evaluation process.

6.6 Limits of authentication assurance

The fact that vulnerabilities do exist in all authentication mechanisms puts a limit on the overall authentication assurance that can be achieved. It also serves to illustrate the diminishing returns to be had in attempting to increase the assurance through increasing the discrimination component of the authentication assurance. Simply increasing password length and complexity will not help if passwords are written down and left where someone else can find them; in fact, it may be counterproductive because the complexity is likely to encourage or necessitate just such an insecure practice. For biometrics, decreasing the false acceptance rate will do little if anything to impact on the susceptibility to spoofing with artefacts. It will, however, bring with it a usability penalty in the form of an increased false rejection rate. If this causes operational difficulties for the application, it may necessitate increasing the false acceptance rate in order to restore the usability.

7 Determining biometric authentication usability requirements

7.1 General

Usability is a blanket term covering a variety of use issues for biometric systems. This can range from complete inability of subjects to use a system successfully to minor ease of use issues. The word accessibility is often used to refer to problems of the ability of subjects to successfully use a biometric system. Reference [8] provides general guidance concerning factors that affect ease of use and accessibility of biometric systems.

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:

— accessibility;

— throughput;

— authentication failure rate for authorized users;

— ease of use at point of authentication;

— ease of use for enrolment.

7.2 Accessibility considerations

Accessibility failures will occur if a subject does not have the biometric characteristic required or if their biometric characteristic properties lie outside the range accepted by the system. It could also occur if the subject is unable or unwilling to present their biometric characteristic to the biometric capture device because of a disability or for some other reason. Accessibility failures can occur at the enrolment stage or subsequently during verification transactions. Accessibility at enrolment and the associated biometric performance parameters and considerations are discussed under the heading “Failure to enrol and exception handling”.

Clearly, if a subject has failed to be biometrically enrolled in a system then biometric verification is not possible thereafter and subject authentication should be provided by alternative means. Some subjects who have been successfully enrolled in the system may still have problems being verified subsequently. This could be for a number of reasons including: differences between the capture device equipment and implementations used at enrolment and verification; differences in presentation of biometric characteristics during enrolment and verification stages; temporary or permanent injury or disability preventing presentation of the biometric characteristic; changes in biometric characteristics due to injury or natural aging. In some cases, re-enrolment may allow the subject to use the system again; otherwise, the subject will need to be authenticated using exception handling procedures. For verification these problems manifest themselves through the occurrence of false rejection errors. If the errors can be contained within acceptable limits and the subject can continue to be verified biometrically, the false rejection errors become a usability issue; if not, the false rejection errors become an accessibility issue.

NOTE A more detailed description of accessibility and associated recommendations are given in Reference [8].

7.3 Throughput

When specifying performance requirements related to throughput, it is important to recognize and differentiate system throughput and biometric throughput. When selecting or specifying the biometric system characteristics, the biometric throughput needs to be decoupled from the impacts of the surrounding system. In many instances, the definition of biometric performance is best expressed as a transaction time rather than a throughput rate (to enable the decoupling). For example, the time required from presenting a biometric characteristic through to the biometric match decision may be followed by a considerable time period to open a vehicle gate, so the dominant influence on system throughput is not the biometric contribution.

The main biometric performance parameters affecting usability from the system viewpoint are the false reject rate and the biometric throughput. There is a relationship between the two because, when a false rejection occurs, the subject will usually be asked to try again, and repeatedly until either authentication is successful or a maximum number of retries has been reached and an exception handling process is invoked. In either case, the biometric throughput will be adversely affected. System throughput is dependent on a number of factors beyond the time taken by the biometric sample acquisition and recognition processes, such as the time for the subject to approach the capture station, for the gates to open and for the subject to move through the gates and release the capture station for the next subject. In many cases, these non-biometric factors will be the major limitations on system throughput.

Different applications will have different requirements on system throughput.

For example, in an employee time and attendance system, the peak load at the start and end of the working day may require a very high system throughput rate.

7.4 Authentication failure rate for authorized users

The quantification of the authentication failure rate for authorized users is most commonly expressed as FRR. The acceptable level of FRR is greatly influenced by the degree of inconvenience caused by such failure. If, for example, a backup procedure is immediately available using an attendant (guard) to perform a photo ID check, then relatively higher levels of FRR may be acceptable. However, if the backup process requires the denied user to traverse to another entry point (possibly quite distant or inconvenient), then the acceptable level of FRR may be very low. This FRR value is adjustable through the use of biometric matching thresholds, but at the expense of changes in FAR, so this should be done in a risk-based manner.

The false rejection rate bears an inverse relationship to the false acceptance rate. Figure 1 shows examples of the Detection Error Trade-off (DET) curve relationship between the false match rate and false non-match rate for two biometric devices as the match/non-match decision threshold is changed (for the purpose of this example, the false match and false non-match rates can be taken as synonymous with false accept and false reject rates respectively). Note that the scales are logarithmic and that the false non-match rate is usually much greater than the false match rate at the normal operating range of the devices. Over this range, the relationship between the false match and false non-match rates is typically fairly linear (on a log/log scale) and the slope shows the degree of dependency; a shallow slope indicates that the false non-match rate is relatively insensitive to changes in the false match rate.

The normal operating range of the device usually corresponds to the shallow slope region of the DET curve where the false match rate is much lower than the false non-match rate. This is a desirable balance for many applications, and it also enables the false match rate to be adjusted to meet varying authentication assurance requirements with minimal impact on the false non-match rate. However, it also means that if the false non-match rate is to be reduced to improve usability by adjusting the decision threshold, this will likely incur a substantial increase in the false match rate.

Persistent false rejections will cause exception processes to be invoked. The occurrence of false rejections is usually not uniformly distributed across the enrolee population. Typically, some enrolees will be found to have relatively high rates of false rejection while others will have relatively low rates. This can be for a number of reasons including the variation in the physical nature of their biometric characteristics (e.g. clear, well delineated fingerprints vs. dry, indistinct fingerprints; clear fully exposed irises vs. irises obscured by drooping eyelids, etc.) and the variation in presentation of the biometric characteristics to the biometric capture device. Some subjects will be more careful and dependable in presenting their characteristics than others. Training can often help to improve presentation but human factors such as personality and motivation will usually intervene to provide some variation in human performance.

The occurrence of persistent false rejections added to those for failure to enrol instances will determine the routine exception handling requirements. The total numbers will of course depend on the user population size. Special factors may be present such as population age or disability that can give rise to higher than normal usability problems, which in turn will affect the exception case volumes.

7.5 Ease of use at point of authentication

Ease of use is a critical consideration for biometric recognition factor selection, particularly from the user acceptance aspect. Biometric recognition factors should be as intuitive as possible, thereby not requiring extensive training or learned skills. The ergonomics of the installation should accommodate the range of the user population, e.g. multiple height or height adjusted face capture cameras. When the biometric system uses cues to direct the user, this interface should be language-independent, possibly based on internationally-recognizable icons or symbols.

NOTE See also ISO/IEC/TR 24714-1:2008, 4.5.2.9 dealing with the ease of use of biometric systems for the subject.

7.6 Ease of use for enrolment

Enrolment in the biometric system should be easy both for the user being enrolled, as well as the enrolling agent. The time required to complete enrolment is often a major driver in decisions to deploy biometric recognition factors. Enrolment policies that are flexible will be beneficial by reducing the number of failures to enrol and the enrolment effort. For example, in a fingerprint system, allow for any one (or two) finger(s) to be sufficient for achieving enrolment, rather than a strict “two index finger” requirement.

7.7 Other aspects of usability

In addition to the FRR level (specified above), other aspects of usability which can be specified in a usability requirements description include the following:

- average transaction duration;
- FTA;
- methods to reduce FRR such as training, signage, subject feedback (at the sensor), ways to encourage habituation;
- dynamic template updating;
- re-enrolment of subjects (periodically or based on trend monitoring and detection of high FRR individuals).

8 Additional considerations in defining biometric security and usability requirements

8.1 Organization of requirements

The main reason for using authentication based on biometric recognition is sometimes related to improving security, for example, to address a security problem with an existing authentication system, although alternatively or additionally it could be to meet specific functional requirements of an application or to improve its usability or the user experience. A clear understanding of the application functionality requirements and the role that biometrics are to play will usually serve to establish the security/usability priorities and to determine what are the performance parameters needed to satisfy the requirements.

The performance requirement specification can best be approached by individually addressing three topics: matching performance, security related requirements, and usability related requirements. The reason that matching performance is treated individually is that the two primary matching performance metrics (FAR and FRR) address security and usability, and are coupled/related by the matching threshold.

As in other fields, authentication security and usability requirements can often conflict and trade-offs may be made to improve usability at the expense of security or vice-versa. However, it is important to understand that authentication security and usability requirements should be determined separately and independently by means of an application risk assessment and management process, and strict limits or “bottom lines” established for security and usability. Trade-offs can then be applied to achieve an optimum balance between security and usability but should never be used to undermine essential security and usability requirements. If it is not possible to achieve a suitable trade off without compromising the essential requirements, this indicates that the proposed authentication solution is not fit for purpose and that further measures are called for.

8.2 Verification and identification modes of operation

The choice between identification and verification modes of operation will often be determined by functionality. If it is desirable for subjects to be authenticated without them providing any prior claim of identity, or if it is necessary to be able to detect attempts by an individual to enrol their biometric characteristics multiple times under different identities, then an identification mode of operation is called for, in the latter example at least for enrolment. Identity mode operation places more severe requirements on false match and false non-match performance parameters, which become progressively more stringent as the number of enrolees in the database increases. For large numbers of enrolees, this often limits the biometric modality chosen to a few highly discriminatory modalities and may additionally need multiple distinct characteristics, e.g. multiple fingers, both irises, or a fusion of two or more modalities. Clearly such implementations will bring with them cost and usability penalties.

Applications with comparatively small numbers of enrolees can often utilize identification mode of operation without undue difficulty. This may be beneficial in simplifying operational use and enhancing user experience, for example to obviate the need for subjects to present additional identification information such as tokens and passwords when using the system.

Many biometric recognition systems use verification mode of operation where the subject claims a specific identity and presents their biometric characteristics for authentication. The acquired biometric sample data is compared with the biometric reference corresponding to the claimed identity and a match/no match decision is made, in turn leading to an authentication/non-authentication decision for the subject. The authentication assurance for a verification mode decision is independent of the size of the enrolee database which usually means that the biometric performance parameter requirements are substantially reduced in comparison with those that would be needed for identification mode operation.

8.3 Stages of authentication

Authentication systems typically have two distinct stages in their operation: an identity proofing stage where the identity of the subject is established and the subject is enrolled in the system and an identity authentication stage where subjects are authenticated by reference to their previous enrolment. Identity proofing is normally a one-off or occasional process, conducted prior to initial enrolment and if re-enrolment is needed for any reason. Identity proofing and identity authentication are distinct activities which may have different performance and usability requirements. With authentication systems based on biometric recognition, this could involve different requirements for biometric modality, error rates, and usability considerations. For example, assurance requirements around enrolment could dictate the choice of modality and performance that would support the searching of a large enrolment database to safeguard against multiple enrolment attempts. These requirements may be unnecessary for subsequent identity authentication transactions. In such cases, an optimum solution might be to use two biometric modalities for enrolment but only one of them for subsequent authentication transactions.

8.4 Authentication assurance and standards

Authentication assurance is really shorthand for the reliance or assurance that can be placed in the decision made by an authentication process. The final authentication decision is binary, i.e. subject authenticated/not authenticated (although the authentication process might involve “fuzzy” intermediate decisions, e.g. uncertain – refer to secondary authentication process). Here, we are not concerned with the internal workings of the process.

Strictly authentication assurance has two components: (a) confidence that a positive authentication decision is correct and (b) confidence that a negative authentication decision is correct. As commonly used, authentication assurance refers to the reliability of the positive authentication decision, i.e. subject authenticated, because the application is usually a logical or physical access control application where the primary security failure is considered to be the admission of an impostor. Note, however, that for some applications the reverse could be the case, where the failure to admit an authorized subject could be a security failure, e.g. a firefighter not admitted to a building to tackle a fire.

Authentication assurance is addressed by International Standards:

ISO/IEC 29115 specifies four authentication Levels of Assurance (LoA). The 4 levels ranging from LoA 1, which represents a minimal confidence in the claimed or asserted identity of an entity provided by the authentication decision, to LoA 4 which denotes a very high level of confidence. The Entity authentication assurance framework provides guidance on selecting an appropriate LoA for an application based on a risk assessment process and the lifecycle management of authentication processes and authentication credentials. While the LoAs defined in ISO/IEC 29115 do not address every conceivable requirement for authentication assurance, they are pitched to meet the majority of requirements in real-world applications.

ISO/IEC 29003 is a companion standard to ISO/IEC 29115. As the title implies, it addresses the initial establishment and confirmation of identity of an entity that takes place prior to the enrolment and registration of the entity into a system or application. Essentially, it handles the requirements for entity authentication assurance before the entity falls within the scope of the authentication assurance regime governed by ISO/IEC 29115. ISO/IEC 29003 defines the identity proofing assurance requirements in relation to the LoAs described in ISO/IEC 29115.

Typically, the identity proofing requirements for an application will match the identity assurance requirements for the application, i.e. the LoAs will be the same; however, there could be exceptions. For some applications, it might be necessary to achieve a high level of assurance at the identity proofing stage, whereas for the subsequent day-to-day authentications the assurance requirements could be lower. This could be the case with large identity management systems where the establishment of “true” identity and the integrity of the enrolment process and enrolment information are of paramount importance, but where subsequent subject transactions have a low level of business risk and value and a lower level of authentication assurance is adequate. In such cases, an optimum business solution might be to impose strict identity proofing requirements (which will likely be costly and time consuming but infrequent), while easing the subsequent authentication assurance requirements for normal day-to-day transactions with consequent cost savings and usability improvements.

8.5 Application-specific performance considerations

8.5.1 Performance for business functionality

The first consideration should be the performance needed to provide the required authentication functionality and maintain the basic operational viability of a business application. If an application needs to be able to distinguish between individuals, the failure to do so will have business consequences. Given that no authentication process will be 100 % reliable and that both increasing the reliability of authentication and dealing with authentication failures will have risk, cost and resource implications, a balance will need to be struck between the two conflicting factors in order to provide an optimum solution from a business viewpoint. Proposed authentication implementation scenarios and associated performance parameters will need to be tested against the business model to demonstrate financial and functional viability, and revised as necessary. The development of a satisfactory business solution will provide basic figures for the performance requirements of the authentication element. In practice, these performance figures will usually translate directly or indirectly into security and usability considerations around the authentication process itself and in turn into technical performance requirements for the authentication mechanisms.

8.5.2 Performance for identity proofing and enrolment

8.5.2.1 General

Identity proofing and enrolment are part of the registration process for subjects who will be authorized to use an application. Identity proofing is the initial stage where the identity of the subject is established to a given level of assurance. Identity proofing often involves trusted 3rd party identity confirmation documents such as birth certificate, passport, utility bills, etc. and personal attestations by trusted persons. Checks may also be done against trusted 3rd party identity databases where a subject has been previously enrolled. Biometrics usually play no part in this except for cases where the trusted third-party information contains biometric data which can be checked against the subject's biometric data.

8.5.2.2 Biometric enrolment

Once the identity proofing checks have established the identity of the subject and the subject is accepted for enrolment and registration in the application, the enrolment process can take place. For biometric enrolment, the subject presents their biometric characteristics and biometric sample data is acquired using a biometric capture station for subsequent enrolment. Typically, biographical identification information will also be recorded alongside the biometric data to identify the subject within the application domain.

The quality of the biometric data acquired during enrolment is important in determining the future performance of the biometric recognition system.[9]. Educating users on the correct and consistent presentation of their biometric samples is recommended. Good quality enrolment data will have a beneficial effect on usability by minimizing the future false rejection rate for the subject. Checking that a subject can verify successfully and easily against their enrolled biometric reference data should be a normal part of the enrolment process. If verification proves difficult or unreliable, the enrolment process should be repeated until reliable verification is achieved. If this is not possible, the subject may be unsuitable for biometric enrolment and will need to be dealt with by an exception handling procedure. Good enrolment practices can also improve FAR. An example of this is enrolling a fingerprint such that the core and delta are captured as opposed to the tip or edges of the fingerprint where there tend to be fewer minutiae.

8.5.2.3 Failure to enrol and exception handling

It may be found that some subjects cannot be successfully enrolled in a biometric recognition system. This could be because they lack the relevant biometric characteristic or because they cannot present their biometric characteristic to the capture device as a result of a disability or possibly because their biometric characteristic lies outside the range that is acceptable to the system. Such enrolment failures will need to be dealt with through the provision of exception handling procedures. Care should be taken to ensure that exception handling procedures do not compromise the authentication assurance requirements for the application; otherwise exception handling may be targeted as an "easy option" by impostors. The volume of exceptions can be gauged from the failure to enrol rate (FTE) performance figure for the biometric enrolment system and the total number of subjects that the application will handle. Note that FTE estimates based on other applications using similar enrolment equipment should be treated with caution because enrolment failure often has demographic dependencies and the demographics of the reference system may not be representative of those of the current system. In practice, enrolment failures are often small in percentage terms and may well be zero for small systems.

8.5.2.4 Multiple enrolment check

In addition to the verification confirmation check during enrolment, some biometric enrolment systems include a check using both the biographic and biometric data that there is not a match with a previously enrolled subject reference. A match could occur for one of two reasons: either the obvious case where the same subject has previously enrolled under the same or a different identity or the case of an apparent match which is in fact incorrect where the biometric recognition process has been unable to distinguish between two (or more) different subjects.

The latter situation is the result of a false match error and will at least lead to the need for further investigation and perhaps to difficulties for an innocent subject, both of which are undesirable outcomes. In small-scale biometric systems (e.g. with fewer than 100 or 1 000 users), the likelihood of a false match will depend on the false match rate (FMR) of the biometric recognition process and of course the number of enrolees in the system. In order to check for multiple enrolment, the biometric recognition process must operate in identification (1:N) mode, which has much more stringent performance requirements than for one operating in verification (1:1) mode. The FMR figure needs to be approximately a factor of N smaller than that for a verification mode operation for the same overall system false match performance (where N is the number of enrolees). Where the number of enrolees is large, other factors need to be considered. However, these are outside the scope of this Technical Report.

A multiple enrolment check is also limited by the false non-match performance figure. In this case, a real match between a subject and a previous enrolment of the subject may be missed as a result of a false non-match error. If, for example, the false non-match rate is 0,5 % there is an average 1 in 200 chance than a subject seeking to enrol multiple times might escape detection by a multiple enrolment check. If this looks poor, we could look at the figure the other way round and note that there is a 99,5 % probability that an attempted multiple enrolment would be detected. This is likely to be a significant deterrent to a would-be multiple enrolee. And of course there may be other non-biometric multiple enrolment checks which would further lower the probability of success.

8.5.3 Performance for identity verification

When operating in verification (1:1) mode, the subject makes a claim of identity (in some cases, the claim of identity could be made in regard to a subject by another person, e.g. a police officer checking whether a suspect is a particular person). The biometric sample acquired from the subject is compared against the previously enrolled biometric reference corresponding to the claimed identity and a match/non match decision is declared. The reliability of the decision is limited by the false match and false non match rates of the biometric recognition process. A false match would result in a subject being incorrectly verified as a different subject whereas a false non match error would mean that a subject failed to be verified as him or herself. For most applications, these represent cases of false acceptance and false rejection respectively, the former normally being regarded as a security problem and the latter a usability problem. In verification mode, the error rates are not dependent on the number of enrolees so, generally, the required FAR/FRR performance figures can be chosen independently of the number of enrolees. Choosing suitable performance figures depends on considerations of security and usability for the application and these are covered in more detail in the following sections.

8.6 Additional security related requirements

In addition to the FAR level (specified above), other aspects of security which can be specified in a security requirements description include the following:

- detection of physical attack/tampering;
- detection of non-zero effort imposter attacks using artefact and other suspicious presentation detection (e.g. patterned contact lenses, disguises);
- methods to mitigate attacks:
  - limit the number of consecutive failed attempts (this can be done overtly, or by notification of a monitoring agent to attempt to apprehend the attacker);
  - force a reject or no-match decision if a sample is a 100% identical match to the enrolled sample;

  - dynamic decision logic to require other authentication mechanisms after failure to match;
- adjustable threshold setting(s) for changes in the threat state (increased alert level).

8.7 Exception handling

Exception handling has already been mentioned previously in reference to accessibility and usability. All authentication processes will be faced with the need to provide exception handling. People forget their passes, tokens and passwords. They will not forget their biometric characteristics but they might not be able to use them either permanently or temporarily. For these individuals, exception handling procedures will be needed. The exact definition of what constitutes exception handling may vary from one system to another, e.g. if a user requires help to use an authentication system, is this exception handling? For an authentication system using biometric recognition, the main performance factors contributing to exception handling are the failure to enrol rate, the persistent false rejection rate and the temporary false rejection rate, these being multiplied by the population size and usage frequency to give volumes. Given accurate performance figures and knowing the size of the user population and the usage profile (uses per day by users), the total volume of exceptions should be a fairly straightforward calculation. Factoring in the usage/time profile will allow peak exception handling rates to be estimated. In practice, there are difficulties. Until a system has been operating for some time, the actual performance figures will not be accurately known. The exception handling volume could be sensitive to the usage by a fairly small number of individuals which could cause the rate to fluctuate significantly as those subjects vary their usage and register for or leave the application. Early exception handling volumes are likely to be above the settled rate because of user unfamiliarity problems and where large numbers of subjects enrol over a short time period (e.g. on the introduction of a new application or system). This will need to be taken into account in the provision of initial exception handling capability.

8.8 Multi-factor authentication

8.8.1 General

Multi-factor authentication can provide a number of benefits such as

- improved discrimination,
- improvements in accessibility,
- improvements in usability, and
- improvements in overall security.

It should be noted, however, that using multiple factors does not mean that all of these improvements can be obtained simultaneously. For example, improved discrimination can be achieved by using two or more factors and combining their outputs using a logical AND. In other words, a positive result will be required from each factor to achieve a positive result overall. This can, indeed, provide improved discrimination but it is likely that a reduction in accessibility will result. Conversely, combining more than one factor using a logical OR function, where a positive result from any individual factor leads to a positive outcome, can provide improved accessibility but with a possible reduction in discrimination.

8.8.2 Improved discrimination

Combining multiple factors such as passwords and biometrics can increase the discrimination of the overall authentication process with attendant gains in authentication assurance. For example, a randomly chosen 4-digit PIN has the ability to discriminate between 10^4 states. This means that using a single guess an attacker would have a 1 in 10^4 probability of defeating the system. Combining this with a biometric recognition system with a false accept rate of 1 in 10^3 would reduce the probability of success using a single imposter attempt to 1 in 10^7, an impressive gain. Obtaining the same improvement using a PIN alone would incur the serious usability difficulty of needing to remember a more complex PIN. There are two important caveats to note; firstly, the two factors should be completely independent and secondly, authentication should be a single indivisible process so that the factors cannot be attacked individually and sequentially.

8.8.3 Improvements in accessibility

For subjects who are unable to use one authentication factor, a choice of authentication factors may enable them to use the system and avoid the need for exception handling. This may be especially useful when using biometric recognition where a choice of biometric characteristic for authentication may allow the subject to access the system as a normal user where otherwise they might have to be dealt with as an exception case. It could also be useful for subjects that, for example, have difficulty remembering passwords who could be offered an alternative means of authentication.

8.8.4 Improvements in usability

Multi-factor authentication can offer usability benefits based on the idea that it is often easier for an individual to perform two or three simple tasks than one complex one. With single factor authentication, achieving increased levels of authentication assurance is often accompanied by usability difficulties, e.g. failure to remember long and complicated passwords; failure to be recognized by biometric systems adjusted to give very low false accept rates. If a single authentication factor can be replaced with multi-factor authentication, the authentication assurance requirements can often be achieved without attendant usability difficulties because each factor can be applied in its operational “sweet-spot”.

8.8.5 Improvements in overall security

All authentication mechanisms have vulnerabilities whether technical, human or procedural. Relying on a single factor for authentication fully exposes the vulnerabilities of the mechanism to attack. Employing multi-factor authentication can provide protection against vulnerability exploits because the vulnerabilities of the various factors lie in different areas and, used in combination, the strength of one factor can cover a weakness in another.

A well-known human/procedural weakness of passwords is the tendency for users to write their password down because of the difficulty in remembering them. This is an obvious vulnerability that can be and is exploited. The addition of a second factor such as biometrics or a token means that even if the password becomes known to an impostor, he/she still cannot succeed without also exploiting a vulnerability of the second factor. This raises the bar in terms of the effort and resources needed to exploit the authentication process as a whole. For this reason, multi-factor authentication is often mandated for applications where higher levels of authentication assurance are necessary (see ISO 29115; LoA 3 and LoA 4). Another example is the potential spoofing vulnerability for biometrics which can be covered by employing a password or token as an additional authentication factor alongside biometric recognition.

Multi-factor authentication can give both breadth and depth to authentication assurance. It can offer a means of breaking through the usual security vs. usability trade-off barrier. However, there are some downsides that need to be considered. Multi-factor authentication is likely to come with a cost penalty in terms of hardware and software. The main cost will be in additional authentication devices, be they biometric capture devices, card readers or password entry devices. And the need for subjects to authenticate using multiple devices will likely reduce throughput for the authentication process where the authentication factors operate sequentially. The effect is difficult to quantify as it will be implementation dependent. Where most of the time is taken with the subject approaching and exiting the authentication station the throughput penalty may be small. If multiple actions can be performed concurrently (e.g. for a face/iris dual-modality biometric system, acquiring the face image at the same time as the iris image), the effect may be minimal.

8.9 Dealing with security and usability shortfalls

It may be found that a proposed authentication solution does not meet both the security and usability requirements of an application. This points to a deficiency in the solution although there could be a strong motivation in such cases to disregard the deficiency and to trade-off security in order to meet the usability objectives (on the grounds that usability shortcomings cannot be hidden and will cause obvious operational problems while security shortcoming will only become apparent if a security breach occurs and is subsequently detected). This is generally not an advisable course of action. The right approach is to look again at the solution to see how the shortcomings may be overcome. For example, a security shortfall in a biometric recognition process might be made up through the use of multi-factor authentication so that the performance requirements on the biometric component can be eased without compromising the overall authentication assurance. Alternatively, improvements in the ergonomic design of the authentication stations may improve the usability without recourse to reducing the security by choosing to use insecure decision thresholds for the biometric recognition.

Nevertheless, if a proposal is to be made to accept lower levels of security than that previously determined and stated in the requirement, this should not be done without a full understanding and assessment of the potential business risks of such a course of action. A resulting security breach could have major or disastrous consequences for a business and the responsibility for the decision will need to be accepted at the highest level in the organization.

8.10 Hypothetical example of quantitative performance requirements

The following hypothetical example is provided to illustrate how the concepts discussed earlier in this Technical Report can be formulated into sufficiently detailed and, in some cases, numerical statements of biometric performance requirements (represented by * in the text below, or $*_1$, $*_2$ where the requirement specifies two performance values). For this example, the application is Physical Access Control (as in 9.3) using a single sample biometric capture device (no fusion) and with an access control policy of 3 attempts per transaction. The system design includes a provision for adjusting to an increased threat level.

MATCHING:

a) Transaction FAR (for zero-effort imposters) < *%

b) Transaction FRR @ FAR of $*_1$% < $*_2$%

c) FNMR (single attempt) < *%

d) For High Threat status, FAR < $*_1$% and FRR < $*_2$%

SECURITY:

a) APCER (attack presentation classification error rate) of *% at an attack potential of medium

b) NPCER (normal presentation classification error rate) of *%

c) Reject any attempt with a perfect match (as indication of a systematic attack)

d) Lockout (for an individual user) after * consecutive failed transactions

   1) Lockout to remain in effect for * minutes

   2) Lockout applies to all entry points

e) FTE < *%

USABILITY:

a) Average transaction time, * seconds

b) Transaction level FTA < *%

c) Individual transaction FRR trend analysis, to detect and require re-enrollment for individuals experiencing > $*_1$% false rejections (using a moving average over the last $*_2$ transactions)

d) Feedback (aural or visual) to subjects when improper biometric presentation is detected (to reduce FTA)

9 Use cases

9.1 General

The following use cases outline requirements – operational business, technical, biometric system, and usability – for representative biometric applications.

9.2 Time and attendance

a) Operational business requirements

   1) Deter labour fraud

   2) Accurate labour accounting (non-repudiation)

   3) Unattended operation

b) Technical requirements

   1) Very high availability

   2) Operability in target environment

   3) Operates in verification mode utilizing a claim of identity (e.g. employee number, read ID badge, etc.)

c) Biometric system requirements

   1) High biometric throughput (especially important if shift-labour)

   2) Very low false rejection rate (acknowledging trade-off with an increase in false accepts due to the low risk/consequence of error)

   3) Very low failure to enrol (secondary procedures for those who do fail to enrol)

d) Usability requirements

   1) Biometric modality selection based on the specific workforce characteristics (e.g. not fingerprints for stoneworker/construction)

   2) Biometric device positioning tailored to the workforce and supportive of high system throughput

   3) Intuitive usage with little training

9.3 Physical access control

a) Operational business requirements

   1) Protect assets within access controlled areas from intruders with malicious intent

   2) Allow access to authorized individuals

   3) Prohibit access for unauthorized individuals

   4) Deter intrusion attempts

b) Technical requirements

   1) Detect intrusion attempts and annunciate an alarm

   2) Operability in target environment

3) Authenticate users at the time and point of access

   i) May involve multiple factors, including biometrics

   ii) Check status of users authority/privilege (including lost/uncontrolled ID tokens, revoked privilege)

4) Operates (usually) in verification mode utilizing a claim of identity (e.g. read from token/ID badge)

c) Biometric system requirements

1) Biometric throughput requirement based on specific conditions

   i) High volume access points dictate more emphasis on high system throughput

   ii) Elevated security access points may warrant trade-off of biometric throughput for lower false accept rate

2) Low false accept rate against zero-effort impostors

3) Detect non-zero-effort imposter and other forms of intrusion attempts (or attack modes using the biometric information)

4) Controlled (and monitored) false rejection rate (acknowledging trade-off with false accepts as thresholds are varied)

5) Low failure to enrol (secondary procedures for those who do fail to enrol)

6) Dynamic template updating to account for characteristic aging

7) Re-enrolment of authorized users with evidence of (1) repeated failures to verify or (2) compromised biometric data

d) Usability requirements

1) Biometric modality selection based on the specific site (or individual access point) characteristics

2) Potential need for non-contact biometric devices in applications with a high degree of hygiene concern

3) Accommodate the range of users in the population considering:

   i) Age

   ii) Anthropometrics

   iii) Disabilities

9.4 Computer sign-on

a) Operational business requirements

1) Protect information assets within computer or network or enterprise

2) Allow sign-on/access to authorized individuals

3) Prohibit sign-on/access for unauthorized individuals

b) Technical requirements

1) Detect intrusion attempts and disable access when repeated attempts exceed policy threshold

2) Authenticate users at the time and point of access

   i) May involve multiple factors, including biometrics

   ii) Check status of user's authority/privilege (including lost/uncontrolled ID tokens, revoked privilege, specific access authority to networks, applications, etc.)

3) Periodically re-authenticate users

   i) To control access to specific information/application based on sensitivity (or need to know)

   ii) To confirm the continued presence of the individual previously verified

4) Operates (usually) in verification mode utilizing a claim of identity (e.g. read from token/ID badge)

c) Biometric system requirements

   1) Low false accept rate against zero-effort impostors

   2) Detect non-zero-effort imposter and other forms of intrusion attempts (or attack modes using the biometric information or result)

   3) Controlled (and monitored) false rejection rate (acknowledging trade-off with false accepts as thresholds are varied)

   4) Low failure to enrol (secondary procedures for those who do fail to enrol)

   5) Modality selection may be driven by IT infrastructure

      i) Workstation/terminal may be equipped with built-in fingerprint sensor or webcam or microphone, requiring no biometric device add-ons

      ii) Installation of peripheral devices (e.g. USB fingerprint reader) or client software may be allowed (or prohibited)

   6) Re-enrolment of authorized users with evidence of repeated failures to verify

   7) Time to sign-on is typically not the driving requirement

d) Usability requirements

   1) For shared use devices, common biometric sensing may be most practical and affordable

   2) For personal-use workstation/PC, the modality or specific authentication approach can be suited to the individual (affordance)

9.5 Remote authentication

a) Operational business requirements

   1) Protect against unauthorized remote transactions utilizing public networks

   2) Allow sign-on/access to authorized individuals

   3) Prohibit sign-on/access for unauthorized individuals

b) Technical requirements

   1) Remote verification of user's claim of identity

   2) Resistance to eavesdroppers

    3) Operates (usually) in verification mode utilizing a claim of identity (e.g. password, account number, etc.)

c) Biometric system requirements

    1) Utilize existing infrastructure (e.g. voice with cell phone, camera embedded on portable multifunction device, etc.)

    2) Enable remote enrolment and centralized enrolment data storage

d) Usability requirements

    1) Limited consideration based on use of personal devices

    2) Suitable for the environment that the user will be exposed to

Annex A
(informative)

Risk assessment

A.1 Analysis of risk and security requirements

To clarify the security requirements, this Annex first describes the scope of the guidelines. After discussing the risks, we will calculate FAR in consideration of the following two viewpoints:

— acceptable risk;

— security level.

A.2 Scope of the guidelines

When estimating the permissible FAR for an authentication system, the guidelines here only consider zero-effort impostor attempts (in which impostors submit their own biometric characteristics as if they were attempting successful verification against their own templates, but the comparison is made against the templates of other users). In other words, the risk of an impostor attempting an illegal access by presenting a faked biometric feature of an enrolled person is excluded. For example, the following risks are also excluded:

EXAMPLE

— A 2D facial authentication system accepts a photo image of an enrolled person;

— A voice authentication system accepts a recorded voice of an enrolled person;

— A fingerprint authentication system accepts a faked rubber fingerprint or a severed finger of an enrolled person.

These problems are closely related to the vulnerability of biometric recognition as an authentication mechanism, and the common concept of FAR is not applicable in most cases. Vendors should inform users of such vulnerability, and users should request that vendors disclose information on vulnerability.

A.3 Assessing risks

A.3.1 Extraction of threats and analysis of their generation probability

The threats to authentication are clarified for some of the use cases described in Clause 9.

A.3.1.1 Physical access control

The following threats exist during authentication in the physical access control use case.

a) Unauthorized access to/extraction of/use of contents of a store for valuables by an unauthorized person

    1) Unauthorized access/extraction/use due to false acceptance by the authentication system

    2) Unauthorized access/extraction/use via tampering with the authentication system

    NOTE 1 Measures for preventing intrusion/extraction (Figure A.1) via a channel other than that protected by the authentication system are needed.

NOTE 2 Some applications may require measures to prevent unauthorized access/extraction/use by a person accompanying an authorized person.

b) Access to a protected space denied to an authorized person

1) Access denied due to false rejection by the authentication system

2) Destruction of the authentication system or access control device by a third party

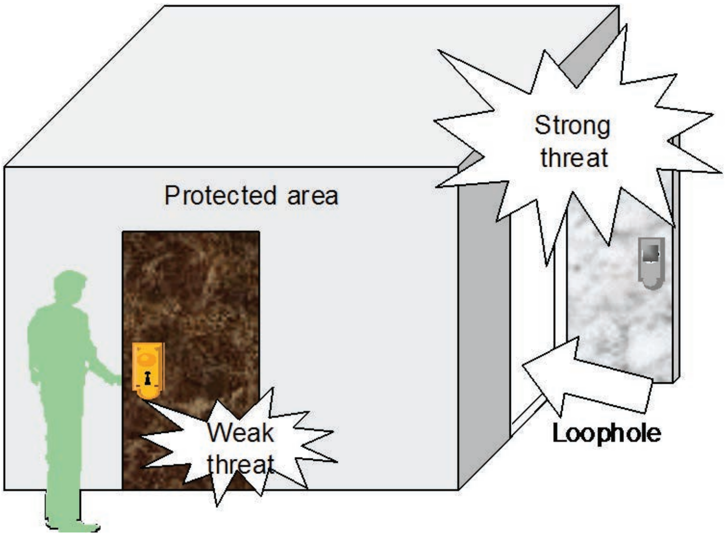


Figure A.1 — Intrusion via loophole

NOTE 3 The threat directly related to the performance requirements that the authentication system has to meet is 1a - Unauthorized access due to false acceptance. The threat of 1 is fraud by a malicious third party who attempts to escape with valuables following unauthorized access. Because impostors use various means of intruding into a storage for valuables, the probability of 1a varies according to their methods. If the system is vulnerable to the threats described in 1b, Notes 1 and 2, then the system is less susceptible to the threats caused by false acceptance in 1a. On the other hand, if the system is resistant to those threats, it is more likely to be affected by false acceptance. This Technical Report only discusses threats to authentication based on biometric recognition, but other threats should be taken into account when considering the total system design.

EXAMPLE With respect to entry control in a complex, an intruder may use an emergency stairway for easy access if security loopholes around stairways or balconies are present.

The overall threat generation probability may be considered similar to crime rate (theft, hijacking, or burglary). It is thus possible to estimate the probability of 1a as part of the overall probability of 1, based on the difficulty of intrusion, extraction, and use of 1b and Notes 1 and 2. In the case of physical access control models, authentication is confirmed in the boundary area of the protected space and thus the probability of unauthorized access via 1b may be regarded as low.

NOTE 4 If any access to the access control device is restricted by a separate means (for example, when access is overseen and confirmed by security personnel), clarify the threat generation probability for the restricted users; this probability might be lower than the average crime rate.

A.3.1.2 E-authentication

The following threats exist during authentication in the e-authentication use case.

a) Unauthorized access to a storage for valuables by unauthorized persons

1) Unauthorized access due to false acceptance by the authentication system

2) Unauthorized access through tampering with the authentication system

NOTE 1 Measures to prevent unauthorized access via security loopholes are required.

b) Access denied to an authorized person

1) Access denied to an authorized person due to false rejection by the authentication system

2) Destruction of the authentication system or access control device by a third person

NOTE 2 As is the case with physical access control, the threat directly related to the performance requirements that the authentication system has to meet is 1a Unauthorized access due to false acceptance. The threats described in 1b and the Notes are those produced by malicious third parties attempting fraudulent access. Since the intention of such intruders does not change from the above-mentioned instance, those threats significantly influence the probability of 1a.

The overall threat generation probability may be considered similar to crime rate (theft, hijacking, or burglary). It is possible to estimate the probability of 1a as part of the overall probability of 1 based on the ease of unauthorized access in 1b and the Notes. In applications that are accessible from the personal space of any user, the probability of unauthorized access according to 1b may be higher.

NOTE 3 Threat generation probability can be estimated from the number of attacks on the electronic access control systems, such as a firewall, or the number of accessible domain users (terminals) coming in through the filters of firewalls.

A.3.2 Estimation of protected value

In this subclause, the value which is to be protected by an authentication system is estimated. The protected value includes all values protected by the application and if possible a value is also ascertained for the threat of fraud.

EXAMPLE Although an ATM contains large amounts of cash, the money potentially exposed to the threat of fraud is only the deposit of an individual customer (or the withdrawal limit per transaction determined by the ATM).

In the case of an application where the involved value cannot be estimated objectively, or there are no records of damages or statistical data, users and evaluators may estimate the amount of involved value.

Secondary damages, such as loss of trust, may be incurred and in some applications these secondary damages should be considered.

In the case of a crime perpetrated for reasons other than profit (the invasion to the system itself being the goal), no apparent damage may occur. In this case, the costs and labour consumed by the resultant investigation, system checks, and preparation of countermeasures should be estimated.

A.3.3 Modelling access routes

As described in A.3.1.1, in applications that use an authentication device, it is important to reduce the frequency of unauthorized access to the device itself. Figure A.2 below shows a model concept of unauthorized access.

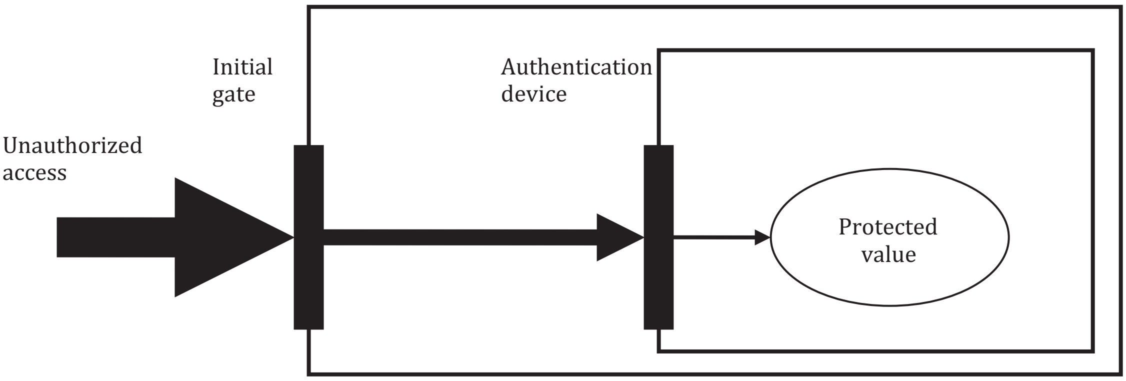


Figure A.2 — Initial gate separate from authentication device

Figure A.2 demonstrates, using arrows of thicknesses that represent the frequency of illegal access, that the frequency of illegal access decreases toward the right, finally reaching the protected value. The initial gate will be the first place to which an indefinite number of people can have access, such as a building entrance or an entrance to a segment, or will be an authentication device in some applications. If the first gate has a guard or a mechanical lock, the frequency of illegal access can be reduced. Authentication using biometric technology will further reduce the frequency of illegal access by screening the access allowed at the entrance. In electronic access control, it becomes possible to screen access by authentication during the transition time from the open menu to the dedicated menu.

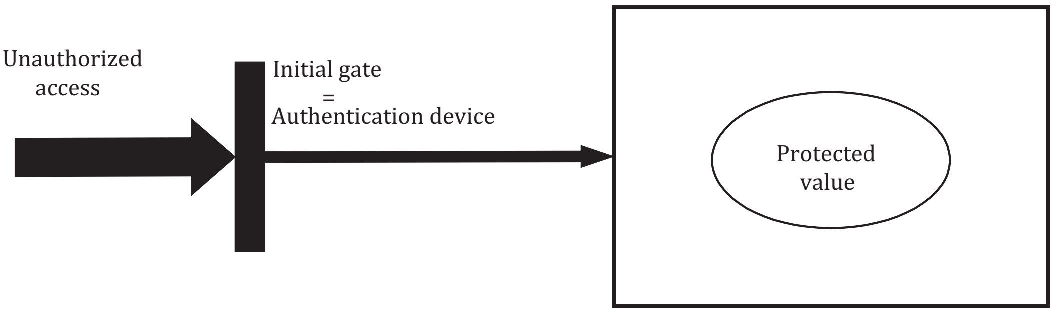


Figure A.3 — Initial gate combined with authentication device

Figure A.3 shows a case in which the first gate serves as the authentication device. As demonstrated here, a very high impostor rejection ability (low FAR) will be required to eliminate illegal access. If a very low FAR is required, no applicable authentication system may exist that satisfies this condition. In electronic access control, authentication may be carried out using an open menu on the World Wide Web (anyone may have access).

A.3.4 Definition of risk

In this Technical Report, risk is defined as possible damages that may occur within a predetermined period of time (such as one year). Such risk is calculated by Formula (A.1), with the protected value and the illegal-access success frequency during the given period used as parameters.

$$(R) = (PV) \times (IASF) \tag{A.1}$$

where

R is the Risk

PV is the Protected Value

IASF is the Illegal Access Success Frequency

EXAMPLE If an application protecting a value of one million yen may allow three illegal accesses per year, the annual risk is calculated to be three million yen.

In transactions in Web trading and EDI, in addition to the risk of false acceptance, the risk of losing opportunities due to false rejection should be evaluated as well. Both risks of losing opportunities due to false rejection and false acceptance should be taken into account in order to calculate potential damages. If the risk accompanying false rejection is large, effective alternative tools will be required.

A.3.5 Formula for IASF (Illegal Access Success Frequency)

IASF at which a biometric system accepts unauthorized access in a given period of time is expressed by Formula (A.2):

$$(\text{IASF}) = (\text{BSIAF}) \times (\text{FAR}) \tag{A.2}$$

where

IASF is the Illegal Access Success Frequency

BSIAF is the Biometric System Illegal Access Frequency

FAR is the False Acceptance Rate

EXAMPLE When a person who is not enrolled attempts to access an authentication system of 0,1 % FAR operating in verification mode 10 000 times claiming the identity of an enrolled person, the system will accept approximately 10 of these claims.

The biometric-system illegal-access frequency (BSIAF) is expressed by Formula (A.3):

$$(\text{BSIAF}) = (\text{IGIAF}) \times (\text{IABMR}) \times (\text{IDR}) \times (\text{NPAA}) \tag{A.3}$$

where

BSIAF is the Biometric System Illegal Access Frequency

IGIAF is the Initial Gate Illegal Access Frequency

IABMR is the Illegal Authentication Block Miss Rate

IDR is the ID Discovery Rate

NPAA is the Number of Possible Authentication Attempts

NOTE This formula relates to the simple situation in which there is only one initial gate. In the real world, many more complex situations are encountered using multiple gates.

The frequency of illegal access to the initial gate (IGIAF) is the frequency of illegal access attempted in a given period of time to the initial gate (see Figure A.3). The initial gate may come in various forms. For instance, in entry control to a computer room, the initial gate may be an entrance to the building in which the computer room exists, the entrance to the floor of the computer room, or a biometric device installed at the entrance to the computer room. The choice of the initial gate will change the means of estimating IGIAF and IABMR, which will be explained next. If the initial gate is an entrance to a building, a certain frequency of illegal access should be expected. In contrast, if a biometric device is the initial gate, the number of people allowed to have access to such a biometric system is limited, so this parameter may be set to a very low value. If it is difficult to estimate an appropriate value for this parameter, the product of the total access (whether legal or illegal) frequency to the gate and the crime rate near the gate can be used.

IABMR is the parameter indicating how many times a security measure fails in blocking impostors at the initial gate to the biometric recognition device. If the initial gate is an entrance and the entrance has a guard, this parameter may be set to a small value. On the other hand, if the initial gate is a biometric recognition device, the value of this parameter is set to 1.

IDR is the probability of the impostor determining the ID number. If the input ID number is exposed to other persons upon authentication and the biometric device is installed in a location to which many people have access, this parameter should be set to a value close to 1. On the other hand, in a system in which the entry of an ID number is made using a hardware token such as an IC card, IDR may be set to a very small value; otherwise, the impostor has somehow obtained the IC card of an enrolled person.

Meanwhile, in a system operated in identification (1:N) mode the imposter does not need to determine a valid ID number, so IDR is set to 1.

NPAA is the number of access attempts allowed per successful authentication, under the assumption that access to the authentication device is finally granted. NPAA can generally be calculated from the sum of the time during which illegal attempts may be made and the time required per authentication (including the response time). For example, if access attempts are allowed with no limitations from midnight to 9 a.m. and each authentication process requires ten seconds, NPAA = 9 × (3 600/10) = 3 240. In practice, NPAA will often be limited by the system security policy, with the user account being disabled and/or a security alert being raised after a pre-determined number of failed attempts.

A.4 Estimation of the permissible FAR from the permissible risk

A.4.1 General

This Clause will explain the procedure for estimating the protected value and permissible risk, as well as the permissible FAR, based on the various parameters discussed in the previous clause.

A.4.2 Estimating the protected value

The protected value is estimated using the method described in A.3.2

A.4.3 Calculating permissible risk

This subclause describes the procedure for estimating the permissible risk that may arise in a given period of time.

If an application is insured, the insurance limit per year can be set as the permissible risk. Otherwise, the permissible risk will need to be evaluated. It is likely to depend on various factors, some of which will be subjective and culturally-determined.

A.4.4 Calculating permissible FAR

If the permissible risk can be calculated in the target application, the permissible FAR can also be calculated by Formula (A.1), Formula (A.2) and Formula (A.3) based on the risk analysis discussion in A.3. For the details of each parameter, refer to A.3.5.

$$(\mathrm{PFAR}) = \frac{(\mathrm{PR})}{(\mathrm{PV})\times(\mathrm{IGIAF})\times(\mathrm{IABMR})\times(\mathrm{IDR})\times(\mathrm{NPAA})} \qquad \text{(A.4)}$$

where

PFAR is the Permissible False Acceptance Rate

PR is the Permissible Risk

PV is the Protected Value

IGIAF is the Initial Gate Illegal Access Frequency

IABMR is the Illegal Authentication Block Miss Rate

IDR is the ID Discovery Rate

NPAA is the Number of Possible Authentication Attempts

Example 1

Suppose that an ATM has an average of 1 000 accesses per day, and that up to one million yen will be lost per successful illegal access. Approximately ten minutes are allowed for each authentication. One session of authentication (ID input, biometric features input and system response) requires 10 seconds. Three million yen is insured per year.

- Estimate of IGIAF at the initial gate

  If the crime rate at the location of the ATM is 1/10 000, the frequency of illegal attempts will be 1 000 × 365/10 000 = 36,5 per year.

- Estimate of IABMR

  This is set to 1, as anyone can have access to the authentication device.

- Estimate of IDR

  This is also set to 1, as IDs may be seen.

- Estimate of NPAA

  In a ten-minute period, NPAA = 600 / 10 = 60 authentication attempts may occur.

Thus, the permissible FAR is calculated as 3 million / (1 million × 36,5 × 1 × 1 × 60) = 0,001 4 = 0,14 %.

NOTE This result is based on the assumption that an average of 0,1 illegal attempts occur per day. However, the permissible FAR will be smaller under either of the following circumstances.

- The authentication device is used in a location with a higher crime rate.
- The monitor is inactive and the allowed time for each illegal authentication is increased.

Example 2

Suppose that there are some terminals for electronic transactions on the first floor of the building of an enterprise. A guard always watches the entrance to the floor, checking every person who enters for an ID badge. Log-in to the terminals is conducted by ten authorized employees, each of whom accesses a terminal using a combination of his or her IC card and biometric recognition. If authentication fails five times consecutively, the authentication system is deactivated for five minutes. If a log-in is successful, up to one million yen can be paid to an account in one session. The permissible loss per year is two million yen.

- Estimate of IGIAF

  It is difficult to estimate the frequency of illegal access to the floor, but it may be set to one per day in order to give a margin to figure. Then, IAF is 365.

- Estimate of IABMR

  Persons other than employees are unlikely to enter the building, as the guard watches every entry. With a good margin and the possibility of internal crime, IABMR is set to 1/100 in order to give a margin.

- Estimate of IDR

  The ID input is conducted using an IC card each authorized person keeps. In consideration of such situations as those in which an authorized employee loses his or her ID card and an impostor steals it, we set IDR to 1/100 with a good margin in order to give a margin.

- Estimate of NPAA

  Based on an estimation of the possible number of access attempts during nine working hours, NPAA is estimated as 9 × 12 × 5 = 540.

Then, the permissible FAR is calculated as 2 million/(1 million × 365 × 0,01 × 0,01 × 540) = 0,10 = 10%.

NOTE This example assumes one illegal access per day at the initial gate. The permissible FAR level is high for the following reasons.

- A guard watches.
- An IC card is used in combination.
- The number of allowable access attempts is limited.

A.5 Estimating the permissible FAR from security levels

Principally, the security requirements for authentication can be calculated by Formula (A.4). Depending on the applications, however, such calculation may be difficult to perform or the risk may be impossible to evaluate in monetary terms. Currently, the security levels that an application must achieve are classified into three levels, and the guidelines for calculating FAR are described for each level.

- **S level**

  This level of security is required in applications in which the potential damages caused by a failure in authentication are extremely high, or in applications that contribute to public security. For example, those for entry control to the Mint Bureau and IC-card issuing facilities, and those used for entry control in nuclear power plants, the defence agency, or police that are deeply involved in public safety.

- **T level**

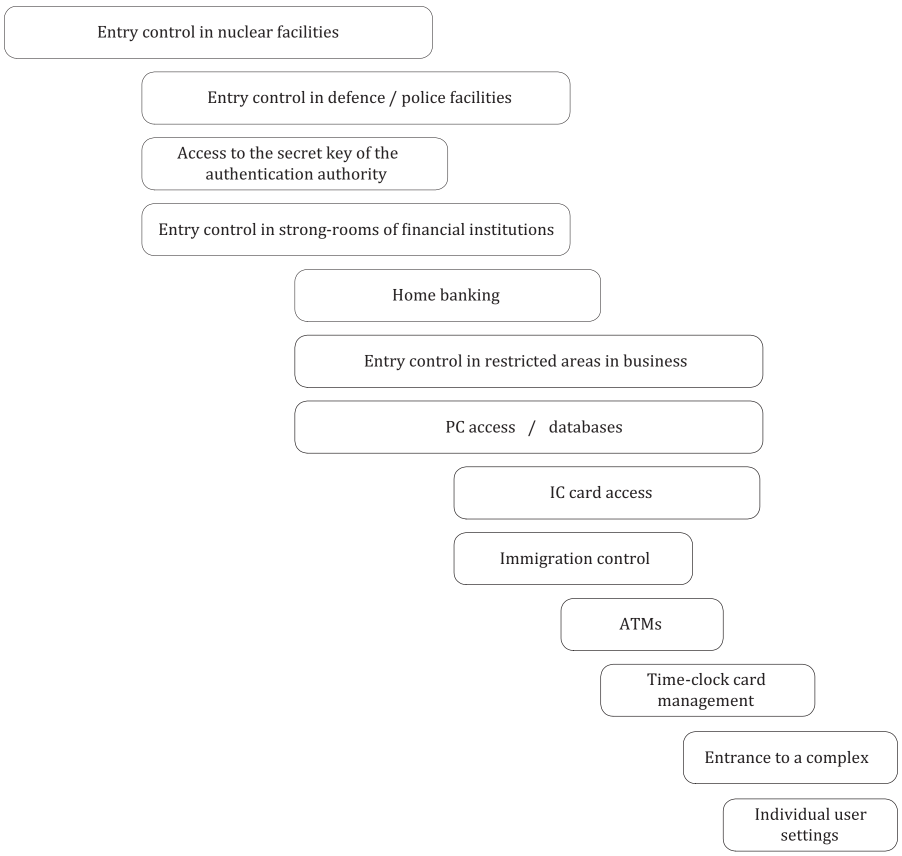
  This level of security is required in applications in which a failure in authentication will cause serious damages or damage social credibility. Those are applications for safe rooms, home banking, ATMs, debit/credit cards, or immigration, electronic patient charts, and databases related to applications which contribute to social credibility. Such applications require both security and convenience.

- **U level**

  This level of security is required in applications in which a failure in authentication will cause a small degree of damages, or those in which there is no need to ensure security, such as PC log-in, entrance to a complex residence, the use of time cards, or customization, fraud monitoring, or terminal management, which place priority on convenience.

Table A.1 is an example. It summarizes possible security levels for each application.

Table A.1 — Classification by security level

	Priority on security		Priority on convenience
Level	High S	Medium T	Base U
Criteria	— Potential damages are very large — Contributes to social safety	— Potential damages are large — Contributes to public trust	— Potential damages are small — Convenience is more important
FAR	0,0001% 0,001%	0,01% 0,1%	1%
Examples of applications			

NOTE 1 FAR differs among applications for the following reasons: 1) the values dealt with in each application vary, and 2) crime rates differ from place to place where the system has been installed. Additionally, in databases, the values of stored data differ, so the permissible FAR levels also differ. In PC access as well, the crime rates vary between a PC anyone is allowed to use and one installed in a room under entry control. The permissible FAR levels change as a result.

NOTE 2 “Individual user settings” refers to customization for individual users to enable easier use. For example, adjustment of driver’s-seat height, video remote-controller settings, air-conditioner settings, and entry to shortcut menus.

Bibliography

[1] ISO 9241-171:2008, *Ergonomics of human-system interaction — Part 171: Guidance on software accessibility*

[2] ISO 9241-210:2010, *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*

[3] ISO 13407,[2] Human-centred design processes for interactive systems

[4] ISO/IEC 29003, *Information technology – Security techniques – Identity proofing*

[5] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[6] ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

[7] ISO/TS 16071,*Ergonomics of human system interaction — Guidance on accessibility for human computer interface*

[8] ISO/IEC/TR 24714-1, *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance*

[9] ISO/IEC/TR 29196, *Guidance for biometric enrolment*

[10] Special Publication 800-63, *Electronic Authentication Guideline, Information Technology Laboratory National Institute of Standards and Technology*, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[11] *Springer Encyclopaedia of Biometrics*. 2009

[12] Palmer A.J *Criteria to evaluate Automated Personal Identification Mechanisms. Comput. Secur.* 2008, **27** pp. 260–284

[13] Statham P. Threat Analysis, *How Can We Compare Different Authentication Methods?* in Biometric Consortium Conference. 2005. Arlington, VA.

[2] Withdrawn.

ICS 35.040

Price based on 40 pages