INTERNATIONAL STANDARD

ISO/IEC 19792

First edition
2009-08-01

Information technology — Security techniques — Security evaluation of biometrics

Technologies de l'information — Techniques de sécurité — Cadre de la sécurité pour l'évaluation et le test de la technologie biometrique

Reference number
ISO/IEC 19792:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19792 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Information technology — Security techniques — Security evaluation of biometrics

1 Scope

This International Standard specifies the subjects to be addressed during a security evaluation of a biometric system.

It covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

This International Standard does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in this International Standard are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme.

This International Standard defines various areas that are important to be considered during a security evaluation of a biometric system. These areas are represented by the following clauses of this International Standard:

— Clauses 4 and 5 of this International Standard give an overview of all terms, definitions and acronyms used,

— Clause 6 introduces the overall concept for a security evaluation of a biometric system,

— Clause 7 describes statistical aspects of security-relevant error rates,

— Clause 8 deals with the vulnerability assessment of biometric systems and

— Clause 9 describes the evaluation of privacy aspects.

This International Standard is relevant to both evaluator and developer communities.

— It specifies requirements for evaluators and provides guidance on performing a security evaluation of a biometric system.

— It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations.

Although this International Standard is independent of any specific evaluation scheme it could serve as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

This International Standard refers to and utilizes other biometric standards, notably those for biometric performance testing and reporting from ISO/JTC1 SC 37. These standards have been adapted as necessary for the specific requirements of biometric security evaluation.

2 Conformance

To conform to this International Standard, a security evaluation of a biometric system shall be planned, executed and reported in accordance with the normative requirements contained herein.

This International Standard describes the specific aspects of a security evaluation of a biometric system in terms of

— statistical error rates (see Clause 7),

— biometric-specific vulnerabilities (see Clause 8), and

— privacy (see Clause 9)

As some evaluation schemes that adopt this International Standard may not address all of the aforementioned aspects it shall further be possible to claim conformance to parts of this International Standard. In this case a security evaluation of a biometric system shall be planned, executed and reported in accordance with a subset of the normative requirements of this International Standard. In this case the requirements that are addressed shall be clearly identified.

Note that conformance to this International Standard is limited to the adoption of the biometric evaluation methodology described and adherence to the specified normative requirements. Conformance does not include scheme related issues such as action to be taken in the event that a system under evaluation fails to meet security relevant evaluation criteria or targets. The overarching scheme is responsible for specifying this action, which could include, for example:

— outright evaluation failure,

— restatement of evaluation criteria or targets to match achieved results, or

— development of a system under evaluation to meet specified evaluation criteria or targets.

3 Normative references

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

ISO/IEC 19795-1:2006, *Biometric performance testing and reporting — Part 1: Principles and framework*

4 Terms and definitions

4.1 General

4.1.1
assurance level
amount of assurance obtained according to the specific scale used by the assurance method

NOTE Definition from [1].

4.1.2
attacker
person seeking to exploit potential vulnerabilities of a biometric system

4.1.3
biometric characteristic
biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

NOTE 1 Definition from [2].

NOTE 2 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 3 Distinguishing does not necessarily imply individualization.

EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm or retinal pattern.

4.1.4
biometric product
biometric component, system or application acting as the scope of an evaluation

4.1.5
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

NOTE Definition from [2].

4.1.6
evaluator
person or party responsible for performing a security evaluation of a biometric product

4.1.7
evaluation
assessment of a deliverable against defined criteria

NOTE 1 Definition from [1].

NOTE 2 In this context, a deliverable is a biometric system.

4.1.8
lamb
biometric reference that results in higher than normal similarity scores on a particular biometric system when compared to biometric samples or references from other subjects

4.1.9
vendor
party that sells, produces or uses a biometric system and is responsible for providing the biometric system and all necessary evidence for evaluation

NOTE In cases where a vendor decides to delegate certain tasks to another party (e.g. to a third party testing laboratory), this party shall be seen as a vendor as well.

4.1.10
user
person interacting with a biometric system

4.1.11
wolf
biometric sample that results in higher than normal similarity scores on a particular biometric system when compared to biometric references of enrolees

4.2 Biometric systems

4.2.1
attempt
submission of one (or a sequence of) biometric samples to the system

NOTE An attempt results in an enrolment template, a matching score (or scores), or possibly a failure-to-acquire.

4.2.2
biometric data
biometric sample at any stage of processing, biometric reference, biometric feature or biometric property

NOTE Definition from [2].

4.2.3
biometric feature
numbers or labels extracted from biometric samples and used for comparison

NOTE 1 Biometric features are the output of a completed biometric feature extraction.

NOTE 2 The use of this term should be consistent with its use by the pattern recognition and mathematics communities.

NOTE 3 A biometric feature set can also be considered a processed biometric sample.

4.2.4
biometric model
stored function (dependent on the biometric data subject) generated from a biometric feature(s)

NOTE 1 Definition from [2].

NOTE 2 Comparison applies the function to the biometric features of a recognition biometric sample to give a comparison score.

NOTE 3 The function may be determined through training.

NOTE 4 A biometric model may involve intermediate processing similar to biometric feature extraction.

EXAMPLE Examples for the stored function could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network.

4.2.5
biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

NOTE Definition from [2].

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch, whorl, and loop types; In the case of facial recognition, this could be estimates of age or gender.

4.2.6
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

NOTE 1 Definition from [2].

NOTE 2 A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database.

4.2.7
biometric sample
analog or digital representation of biometric characteristics prior to biometric feature extraction and obtained from a biometric capture device or biometric capture subsystem

NOTE 1 Definition from [2].

NOTE 2 A biometric capture device is a biometric capture subsystem with a single component.

4.2.8
biometric template
set of stored biometric features comparable directly to biometric features of a recognition biometric sample

NOTE 1 Definition from [2].

NOTE 2 A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced or compressed form, is not a biometric template.

NOTE 3 The biometric features are not considered to be a biometric template unless they are stored for reference.

4.2.9
enrolment data record
record created upon enrolment, associated with an individual and including biometric reference(s) and typically non-biometric data

NOTE Definition from [2].

4.2.10
transaction
sequence of attempts on the part of a user for the purposes of an enrolment, biometric verification or biometric identification

NOTE There are three types of transaction: an enrolment sequence, resulting in an enrolment or a failure-to-enrol; a verification sequence, resulting in a verification decision; or an identification sequence, resulting in an identification decision.

4.3 Biometric processes

4.3.1
authentication
provision of assurance of the claimed identity of an entity

NOTE Definition from [1].

4.3.2
biometric application decision
conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data

NOTE 1 Definition from [2].

NOTE 2 Biometric application decisions can be made on the basis of complex policies, allowing for variable numbers of positive comparison decisions.

NOTE 3 A biometric verification application could allow a positive biometric application decision even if there are one or more non-matches against enrolled biometric references.

EXAMPLE A biometric application decision could be “accept claim”.

4.3.3
biometric recognition
recognition using a biometric product

NOTE A biometric recognition can either be realized as a biometric verification or as a biometric identification process.

4.3.4
comparison score
numerical value (or set of values) resulting from a comparison

NOTE Definition from [2].

4.3.5
de-enrolment
deletion of the biometric reference from storage and if necessary, associated data in connection with the end-user's identity from the biometric system

4.3.6
decision policy
collection of parameters, rules and values used to determine the acceptance or rejection of the biometric recognition of the subject

4.3.7
enrol
create and store an enrolment data record for a biometric capture subject in accordance with an enrolment policy

NOTE Definition from [2].

4.3.8
enrolment
action of enrolling or being enrolled

NOTE Definition from [2].

4.3.9
biometric identification
biometric system function that performs a one-to-many search to obtain a candidate list

NOTE Definition from [2].

4.3.10
comparison decision
determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs

NOTE 1 Definition from [2].

NOTE 2 A match is a positive comparison decision.

NOTE 3 A non-match is a negative comparison decision.

NOTE 4 A decision of “undetermined” can sometimes be given.

4.3.11
threshold
boundary value of the comparison score used by the comparison application to automatically generate the matching decision

4.3.12
biometric verification
biometric product function that performs a one-to-one comparison

NOTE Adapted from [2].

4.4 Error rates

NOTE Definitions 4.4.1 to 4.4.9 and 4.4.11 are from ISO/IEC 19795-1:2006.

4.4.1
active impostor attempt
attempt in which an individual tries to match the stored template of a different individual by presenting a simulated or reproduced biometric sample, or by intentionally modifying his/her own biometric characteristics

4.4.2
failure-to-enrol rate
FTE
proportion of the population for whom the system fails to complete the enrolment process

NOTE The observed failure-to-enrol rate is measured on test crew enrolments. The predicted/expected failure-to-enrol-rate will apply to the entire target population.

4.4.3
false non-match rate
FNMR
proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample

NOTE The measured/observed false non-match rate is distinct from the predicted/expected false non-match rate (the former may be used to estimate the latter).

4.4.4
false match rate
FMR
proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template

NOTE The measured/observed false match rate is distinct from the predicted/expected false match rate (the former may be used to estimate the latter).

4.4.5
false reject rate
FRR
proportion of verification transactions with truthful claims of identity that are incorrectly denied

4.4.6
false accept rate
FAR
proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

4.4.7
identification rank
smallest value k for which a user's correct identifier is in the top k identifiers returned by an identification system

NOTE The Identification rank is dependent on the size of the enrolment database, and should be quoted “rank k out of n”.

4.4.8
pre-selection algorithm
algorithm to reduce the number of templates that need to be matched in an identification search of the enrolment database

4.4.9
pre-selection error
⟨pre-selection algorithm⟩ error that occurs when the corresponding enrolment template is not in the preselected subset of candidates when a sample from the same biometric characteristic on the same user is given

NOTE In pre-selection that is based on building partitions/classes of users, pre-selection errors happen when the enrolment template and a subsequent sample from the same biometric characteristic on the same user are placed in different partitions.

4.4.10
test crew
set of test subjects gathered for an evaluation

NOTE Definition from [1].

4.4.11
zero-effort impostor attempt
attempt in which an individual submits his/her own biometric characteristics as if he/she were attempting successful verification against his/her own template, but the comparison is made against the template of another user

4.5 Statistical

4.5.1
confidence interval
lower estimate L and an upper estimate U for a parameter x such that the probability of the true value of x being between L and U is the stated value (e.g. 95 %)

[ISO/IEC 19795-1:2006, definition 4.8.2]

NOTE A confidence interval is always associated with a corresponding stated value of probability. In this International Standard the stated value of probability is termed “confidence value”

4.5.2
confidence value
stated value of probability corresponding to a specified confidence interval

5 Abbreviated terms

DET detection error tradeoff (curve)

FAR false accept rate

FDIS Final Draft International Standard

FMR false match rate

FNMR false non-match rate

FRR false reject rate

FTE failure-to-enrol

IS International Standard

6 Security evaluation

6.1 Overview

This clause further delineates the scope of this International Standard described in Clause 1 and provides a context in which the security evaluation of biometrics is conducted.

Figure A.1 shows the reference architecture of a biometric system used in this International Standard. A biometric system comprises a collection of hardware and software components. It is normally used to implement a biometric application, in which case it operates in an externally provided environment that forms an essential part of the application. The environment comprises not only physical factors such as space, temperature, humidity, illumination, etc., but also all procedural aspects and human users of the system. Users of the system comprise all classes of people who might interact with the system such as operators, administrators, enrolees, impostors etc.

This International Standard is principally directed at the security evaluation of biometric systems themselves rather than complete biometric applications. A biometric application comprises a biometric system and possibly other hardware and software components, together with an operating environment, organisational processes and policies that collectively provide the functionality of the application. These additional elements may have security vulnerabilities of their own or might amplify or mitigate vulnerabilities possessed by the biometric system itself.

Vulnerability assessment should be conducted in an ordered manner that will involve the investigation of individual component vulnerabilities. Evaluators should, however, exercise caution when assessing the results of component vulnerability assessment without considering the interactions that take place with other system components. These interactions can determine whether or not component vulnerabilities can be exploited in practice. Therefore evaluators should always assess vulnerabilities in the context of the overall system functioning and not solely based on assessment of individual component vulnerabilities.

Similarly, a biometric system may display intrinsic vulnerabilities that are realised, aggravated or mitigated by interaction among system components. For example, a biometric comparison algorithm may display anomalous behaviour if presented with out of range biometric data, and this behaviour could give rise to a vulnerability. However, if the component(s) responsible for supplying the biometric data to the comparison algorithm prevents such anomalous data being supplied, there is no resultant vulnerability. Although the methodology in this International Standard could be used to evaluate security factors for components of a biometric system, evaluators should exercise caution when examining individual component vulnerabilities and seek to understand the interactions between components to determine how these may affect the resulting system vulnerabilities. In general the assessment of individual component vulnerabilities may have limited value and be misleading if conducted outside the context of a system evaluation.

This International Standard specifies a methodology for the evaluation of the technical security of biometric systems. It does not seek to address the broader issues of security evaluation of a complete biometric application. Accreditors of biometric applications will therefore need to develop threat/risk models for applications and to assess whether other non-biometric specific vulnerabilities exist in the overall system and what effect any biometric vulnerabilities discovered may have on the overall system security.

6.2 Methodology

This International Standard addresses the aspects of security evaluation that are specific to biometric systems. A biometric system security evaluation will probably also involve the evaluation of IT security aspects. This International Standard does not cover these aspects and evaluators should refer to other IT security evaluation standards and methodologies for the evaluations of non-biometric aspects of a system security evaluation, e.g. Common Criteria ([3]).

The vendor of the biometric system under evaluation will have to provide a description of the system before an evaluation can begin. This will allow the evaluator to become familiar with the system and support decisions later in the evaluation process. The biometric-specific aspects of biometric system security evaluation described in this International Standard are:

— Measurement of statistical error rates (see Clause 7)

— Biometric specific vulnerabilities (see Clause 8)

— Privacy (see Clause 9)

The underlying concept of this methodology is that – apart from these three areas – a security evaluation of a biometric system can be conducted in the same manner as the security evaluation of any other IT system.

Clause 7 introduces the concept of a test of security-relevant error rates in the context of a biometric system security evaluation. Statistical error rates can be measured for biometric algorithms alone (typically using pre-existing databases of biometric samples), or for systems where users provide the biometric samples directly to the sensor of the data capture component. Error rate testing of biometric algorithms is often used to compare the performance of different algorithms and to quantify changes resulting from algorithm development. Algorithm testing is of limited value in security evaluation because algorithmic errors are only one source of errors in a biometric system. It is normally necessary to conduct statistical error measurement of biometric systems using biometric samples acquired by the capture component of the system from real subjects in a scenario test. However, a statistical test of an algorithm may contribute to the necessary understanding of the biometric system that is needed to prepare the test or to find a claim about the maximum error rates of the biometric system.

Clause 8 provides guidelines for vulnerability assessment. Technical vulnerabilities are dealt with under headings that correspond to potential vulnerabilities of biometric systems, based on theoretical considerations and practical experience. The exploitation of a potential vulnerability will typically involve multiple components. For example, a spoof artefact will need to be accepted by the sensor and defeat any spoofing prevention; pass the acquisition quality analysis step; be successfully pre-processed and feature extracted and pass any subsequent quality control check. These steps will normally involve more than one component of the system.

Clause 9 details evaluator actions required to address the concerns of privacy when processing and storing biometric data. This is an inherent security concern for biometric systems because the data used for authentication is personal and may be governed by constraints of use determined by legislation or codes of practice in various countries.

This International Standard defines vendor and evaluator roles and specifies requirements and actions for each party. Although the methodology is scheme-independent, the separation of roles here reflects the perceived need for the responsibilities and actions of the evaluator to remain independent from those of the vendor.

7 Error rates of biometric systems

7.1 Introduction

One inherent characteristic of biometric recognition is that the decision of the biometric system is subject to errors that can be expressed in terms of statistical error rates– for example: false accept and false reject rates. These and other performance parameters also have implications for the strength of security provided by a biometric system when used for authentication.

Hence each security evaluation of a biometric system shall include an assessment of the security-relevant error rates.

The testing and reporting of security relevant error rates in this International Standard is based on ISO/IEC 19795-1:2006. This International Standard utilises elements of biometric performance and performance testing and reporting that are relevant to biometric security evaluation.

7.2 Concept – Testing security-relevant error rates

The reliability of the biometric verification or identification functionality of a biometric system is an important factor that determines the confidence that can be placed in an authentication decision provided by the system. This reliability can be measured by means of a properly conducted test of the system performance parameters that are relevant to authentication assurance. For an access control system, these parameters include the False Accept Rate (FAR) and False Reject Rate (FRR), and their close relatives False Match Rate (FMR) and False Non-Match Rate (FNMR) (see 4.4 and ISO/IEC 19795-1:2006 for a detailed definition of and differentiation between these terms).

The reason why both FAR/FMR and FRR/FNMR need to be measured is that there exists an inverse relationship between these types of error for a biometric system and it is usually possible to adjust the system to achieve any desired FAR/FNMR value if no limitation is placed on the FRR/FNMR value. For an access control application the FAR/FMR value can be thought of as denoting the security while the FRR/FNMR value corresponds to usability. This security/usability trade-off is analogous to the case of passwords where password length and randomness (security) can be traded off against difficulty of memorising (usability). Many password security policies are formulated by consideration of the security aspects alone, without regard to usability. This is not, however, deemed acceptable for a biometric system. The reason for this apparent inconsistency is perhaps that a usability failure for password authentication is seen as a human failure, whereas for biometric recognition it is seen as a system failure.

The purpose of measuring security relevant error rates of a biometric system is to provide reliable figures upon which to establish the fundamental assurance of verification or identification decisions made by the system.

The test of security relevant error rates starts with a security claim based on meeting or bettering specified error rate limits. The performance test then aims to substantiate or refute this claim. In addition, evaluators may need to consider the possible effect of test users having special characteristics or non-random choice of test users on performance, and hence security.

The approach for testing described in this clause is based on a six step concept:

1) The vendor shall supply a description of the system and the context of its use (see 7.2.1).

2) The vendor shall claim the maximum values for the security-relevant error rates (see 7.2.2).

3) The claims shall be checked by the evaluator (see 7.2.3).

4) The vendor shall perform a test to prove that the claim is correct, i.e. that the error rates meet the claim (see 7.2.4).

5) The vendor's test shall be assessed by the evaluator (see 7.2.4).

6) The evaluator shall perform an independent test (see 7.2.5).

These steps will be introduced in more detail in the following subclauses.

7.2.1 System description (Step 1)

The vendor shall provide the evaluator with a description of the biometric system under evaluation and its context of use.

This description shall contain the following:

— a description of the intended use of the system,

— information on whether the product is intended to perform biometric verification or identification,

— a description of the intended environment of the system,

— a description of the target population of the system,

— a description of all security relevant configuration parameters (including all threshold settings) and their recommended settings to achieve the performance claims for the intended environment and target population (see 7.2.2).

This description of the system is important for the evaluator in order to decide upon further requirements in the context of this International Standard.

7.2.2 Vendor claim (Step 2)

The vendor shall provide performance claims in the form of a set(s) of maximum values of security-relevant error rates that can be achieved simultaneously. For each claimed value of a security relevant error rates the vendor shall provide the threshold(s) that the claim bases on.

This requirement comprises three aspects:

— The vendor shall perform and provide an analysis of which error rates of the biometric system are security-relevant.

— The vendor shall provide the evaluator with set(s) of maximum values of security-relevant error rates that can be achieved simultaneously in the context of relevant configuration parameters as defined in 7.2.1.

— The vendor shall provide justification as to why the maximum values for security-relevant error rates are acceptable considering the intended use of the biometric system.

7.2.3 Examination of vendor claim (Step 3)

The evaluator shall determine whether the list of security-relevant error rates is complete and whether the claim for the maximum values of the error rates is adequate. They must also check the vendor's justification of the error rates that the vendor considers to be irrelevant.

Factors that should be considered when deciding whether the claim for the maximum values of error rates is adequate include:

— the (future) application case of the biometric system and its security needs,

— legal requirements,

— contractual requirements (or customers' requirements),

— requirements resulting from a specific evaluation methodology which is used.

Please note that, during a security evaluation, it is not the responsibility of the evaluator to decide whether the claim of the error rates and their maximum values meet the “state of the art” of a biometric technology i.e. whether the biometric system would in theory be able to meet better claims. The relevant question for this aspect should rather be whether the vendor's claims meet the needs of the customer in the context of the future application of the biometric system.

The evaluator shall consider all error rates in ISO/IEC 19795-1:2006 during their analysis to evaluate whether the list of identified security-relevant error rates is complete.

To ensure that the list of error rates is complete the evaluator will have to decide for each error rate that is defined in ISO/IEC 19795-1:2006 whether it is relevant for the biometric system under evaluations. Primarily each error rate should be considered to be relevant.

Obvious reasons for which an error rates may not be relevant include:

— specific legal requirements that do not require this error rate,

— an error rate that is only applicable to a biometric identification system, where a biometric verification system is being evaluated,

— the pre-selection error rate in systems that do not perform pre-selection.

If the vendor considers a certain error rate to be irrelevant to security and this is not apparent to the evaluator, the vendor shall provide additional justification to satisfy the evaluator. Otherwise the vendor shall provide the error rate value(s) for the error rate under consideration.

7.2.4 Vendor test and evaluation of vendor test (Step 4 and 5)

While the previous clauses each addressed one step of the six test approach as introduced in 7.2, this subclause combines the requirements for two steps of the approach:

— The vendor's test to prove that the claimed error rates are correct, i.e. the error rates meet the claim.

— The evaluator's assessment of this test.

This is beneficial to the interests of clarity and conciseness as the requirements for vendor and evaluator testing share many common features. Where differences do occur they will be indicated. Note that if specific scheme requirements require the vendor and evaluator actions to be separately documented, it may be necessary to split the information in this clause into 2 distinct subclauses

The vendor shall plan, conduct and document a test which substantiates the claimed security relevant error rates. This test shall comply with relevant parts of ISO/IEC 19795-1. The evaluator shall check and validate the vendor test.

NOTE The requirements for vendor testing do not prevent the task being entrusted to a third party test organization. However, such an organization shall be independent from the evaluator reviewing the test.

The role of performance testing in a biometric security evaluation is to determine or validate claimed security-relevant error rates. Evaluations carried out according to this International Standard are required to conform to the performance testing and reporting standards specified in ISO/IEC 19795-1:2006. In addition, the following subclauses (7.2.4.1 to 7.2.4.8) are normative for tests conformant to this International Standard. Those requirements extend, limit or emphasize requirements given in ISO/IEC 19795-1:2006. In the event of conflicting requirements, the requirements in this International Standard shall take precedence.

NOTE Performance testing requires significant resources. It is therefore advisable for the vendor and evaluator to agree the test methodology, protocol and report format prior to commencing the performance test, to ensure that the performance test will meet the requirements of the evaluation.

In addition to the requirements from ISO/IEC 19795-1:2006, the following issues shall be addressed during planning and execution of testing and shall be included in test documentation:

— Any assumptions made about the test scenario shall be stated and justified,

— The test crew shall be appropriate to the target application,

— The test environment shall be consistent with the target application,

— The security relevant error rates shall be reported and shown to be acceptable for the target application,

— Security relevant threshold value(s) and configuration parameters shall be set in accordance with vendor recommendations for the test,

— The retry counter shall be set in accordance with the vendor recommendations,

— The single attempt error rate shall be measured and reported,

— The statistical approach to the test shall be reported and justified by the vendor.

Additional information about these requirements can be found in the following subclauses.

7.2.4.1 Assumptions

During each test of the security relevant error rates of a biometric system assumptions must be made in order to design an appropriate test scenario.

The vendor shall report all assumptions which have been made during the design and test phases.

Assumptions traditionally address:

— the intended environment of the biometric system,

— the expected behaviour of intended users of the biometric system,

— the expected behaviour and background of attackers who might attack the biometric system in its intended operating environment.

How closely the test conditions and assumptions match the intended operational conditions will affect how reliably the test results will predict the operational performance of the biometric system. The vendor should report all necessary assumptions made for the test, ensure that those assumptions are consistent with the intended usage of the biometric system, and ensure that the test design assumptions will yield reliable results. Moreover, the vendor should provide information about the system behaviour in the event of unexpected users (i.e. users who do not fit into the target population of the system). This information will be considered in the context of vulnerability assessment.

The evaluator shall analyse the vendor-provided assumptions in order to verify that:

— all necessary assumptions have been reported by the vendor,

— the assumptions are consistent with the intended usage of the biometric system as reported by the vendor,

— the test design is consistent with the assumptions so that the test results will be reliable.

7.2.4.2 Test crew

The test crew used for evaluation shall be

— representative of the target population of the biometric system, and

— big enough to provide the required statistical confidence in the results.

The demographic profile of the test crew should closely match that of the target population. Any deviation from this condition will reduce the confidence that can be placed in the test results. The vendor shall identify any characteristics of the test crew which may bias the security-relevant error rates. Additionally, the vendor shall report the distribution of those identified characteristics among the test crew and the target population of the biometric system. This analysis may base on the hypothetical target population as reported by the vendor.

It should be noted that it is the responsibility of the evaluator to decide whether the identified deviations of the test crew are complete and acceptable. As this International Standard is independent of any concrete evaluation methodology and the degree of deviations that may be acceptable for a certain test design also

depends on the confidence that has to be achieved by the test, defining concrete limits on such deviations is beyond the scope of this International Standard.

The principal issues that determine the necessary test size of a test crew are:

— the necessary degree of confidence (given by the concrete confidence value and confidence intervals),

— the error rates (lower error rates usually require a bigger test size), and

— the design of the test (e.g. whether multiple transactions are allowed per user).

In performance testing, the error rates of a biometric system being tested are often unknown prior to the test. In such a situation, the necessary test size can only be estimated (based on the expected error rate), and the confidence value resulting from the test is calculated after the test has been conducted.

However, during a security evaluation according to this International Standard, a claim of the maximum values of error rates will be available and this claim – together with the test design and the necessary confidence that has to be achieved by the test – can be used to determine the necessary size of the test crew.

Additional guidance on how to determine the necessary test size can be found in ISO/IEC 19795-1:2006.

Also, the behaviour of the test crew in regard to their cooperation and care they take in presenting their biometric characteristics to the data capture subsystem will affect the error rates measured. Therefore it is an important aspect of a representative test crew that their behaviour closely matches that of the target population if the test results are to be a reliable predictor of the operational results. Consideration needs to be given to:

— cooperation and motivation of the test crew, and

— familiarity of the test crew with the use of the biometric system.

The test crew must be given appropriate instruction, training and motivation to ensure that their behaviour matches that of the intended target population.

Operator actions and the overall conduct of transactions shall also be given due consideration to identify factors that may affect error rates (e.g. sensor cleaning policy). The test scenario shall emulate the operational scenario in all respects that may affect system error rates.

It is known that the conditions of the enrolment process for the test crew and the corresponding policies have a significant impact on the error rates of the biometric system. The conditions of the enrolment process used for testing shall closely match the operational conditions of the biometric system.

Any procedures used to select the test crew shall be stated. The Failure to Enrol Rate shall be reported along with the other required test results.

Note that error rate tests using impostors selected because their biometric characteristics are known or believed to have special properties leading to an increased likelihood of false acceptance are dealt with as part of vulnerability assessment in Clause 8. However, the vendor may decide to combine tests including a set of users who are not representative of the target population of the biometric system with this test.

7.2.4.3 Environment

The environmental conditions for the vendor's test shall be as close to the conditions of the intended environment as possible.

This requirement ensures that the environmental conditions of the test emulate the intended environment. In case of environmental differences, the vendor shall present an analysis showing that the differences did not influence the test results. Note that the question of whether different environmental conditions may deteriorate

the security-relevant error rates will also be addressed in the context of vulnerability assessment (see Clause 8).

All environmental conditions relevant to the test scenario shall be recorded and reported. Additionally, the intended environment for the biometric system shall be reported together with the evaluation results.

The explicit requirement on reporting the intended environment together with the test result exists in order to enable customers of the biometric system to ensure that they operate the biometric system within an appropriate environment.

7.2.4.4 Related error rates

If a measured error rate is dependent directly or indirectly on other error rate(s), the corresponding values of those other error rates shall be specified and reported.

This requirement is present to obviate the possibility of an unrealistic error rate claim being made that depends on unreasonable values for related error rates(s) via the decision policy.

For example tuning a biometric system to meet a claim of a certain FAR will lead to a certain FRR (as FAR and FRR correlate). Such tuning falls into the responsibility of the vendor and is an important feature to allow the use of the same biometric system for different application cases. However, when using unreasonable values for a decision policy, the resulting tuning for a certain FAR may lead to a FRR that makes the system unusable.

While the requirement that the related error rate has to be tested and reported in such cases cannot prevent a vendor from tuning the system, it will make such tuning efforts and their effect visible and leave the decision of whether to use the biometric system at the threshold setting(s) used in the test to the customer. If a full DET curve is available from the test, a customer could choose to use the system at a different threshold setting(s).

7.2.4.5 Decision policy and threshold settings

All reports of error rate claims and measurements shall include details of the corresponding decision threshold(s) settings used and, where relevant, any quality threshold criteria employed.

General performance testing usually results in the generation of a DET curve showing the relationship between the error rates (e.g. False Match Rate and False Non-Match Rate) as the Match/Non-Match decision threshold is changed. For a security evaluation, however, testing may be conducted for only one or a few decision threshold values that correspond to specific vendor claims regarding error rates.

While this may help to reduce the effort for the necessary tests, it also means that a biometric system that has been tested this way may only be operated using the recommended operating points, as the test cannot provide any statement about the security-relevant error rates outside these operating points. Therefore, generating and reporting the complete DET curve, thereby allowing users to estimate the performance that can be achieved at other threshold settings, should be considered if a full DET curve can be generated with little additional effort.

7.2.4.6 Retry counter

Biometric systems often allow multiple attempts at recognition for a single transaction. This is usually to improve the usability of the system by reducing the False Rejection Rate. However, allowing multiple attempts may also have the undesirable side effect of slightly increasing the False Accept Rate. A maximum limit on the number of attempts allowed is usually imposed to prevent exhaustion attacks, particularly in cases of unsupervised operation. This is often implemented by means of a retry counter with a limit count for a single transaction. Note that it is also usually necessary to impose a timeout limitation to terminate a transaction in cases where the subject ceases recognition attempts before the retry counter limit is reached.

The retry counter generally controls only the maximum number of recognition attempts. The typical scenario is that the subject makes a first attempt. If recognition is successful, the transaction terminates successfully. If not, a second attempt is allowed which, if successful terminates the transaction successfully. Otherwise

further attempts are allowed until the retry limit is reached, whereupon the transaction terminates unsuccessfully.

In operational use there will typically be a mix of 1, 2, ..m attempt transactions (where m is the retry limit). The subject will usually be aware whether or not they have been successfully recognised at each attempt. This is relevant because the performance (error rates) of the system is usually influenced by subject behaviour as well as technical capability. It is therefore important that the test scenario simulates as closely as possible the operational scenario if the test results are to be reliable predictors of operational performance.

If a biometric system has a mechanism to limit the maximum number of failed (sequential) attempts, the vendor shall provide the description of this mechanism and the recommendations for its settings. The description shall also describe what happens when the maximum number of attempts is exceeded.

The vendor shall test and report the error rates under consideration of the retry counter setting.

NOTE This requirement does not mandate that the full number of attempts that is allowed has to be exhausted in every transaction of the test but primarily defines the maximum number of attempts during testing. It further shall oblige the vendor to report the results in accordance with the settings of the retry counter. As an example it must not be possible to test and report a False Reject Rate for four attempts if the tested system will only allow three attempts in later operation.

During their analysis, the evaluator will examine the described mechanism and check the settings for a retry counter to be appropriate for the application case of the biometric system.

If a biometric system has no retry counter, the vendor will have to provide the evaluator with a justification of why such a mechanism is not necessary. A possible justification for a missing retry counter may be that it is not possible to perform many attacks against the biometric system (e.g. due to an assumption of a guarded environment) or that the defensive measures taken when the retry counter threshold is exceeded may open the path to denial of service attacks.

Retry counters are typical mechanisms of biometric verification systems. For a biometric identification system, the simple retry counter approach is not applicable, as successive attempts cannot be assumed to come from the same individual. However, equivalent mechanisms may be implemented (e.g. a check on successive similar — but not successfully matched — probe samples). Those equivalent mechanisms shall be considered for this requirement in the same way as standard retry counters.

7.2.4.7 Single attempt error rate

In operational use a biometric system will typically be a mix of 1, 2, ..m attempt transactions (where m is the retry limit as described in 7.2.4.6). The user is usually aware of whether or not they have been successfully recognised at each attempt. This is relevant because the performance (error rates) of the system is usually influenced by subject behaviour as well as technical capability. It is therefore important that the test scenario simulates the operational scenario as closely as possible if the test results are to be reliable predictors of operational performance.

However, the corresponding error rate for a single attempt is an important mean to make evaluations of biometric systems comparable.

Regardless of the transaction and decision policy, the vendor shall also test and report corresponding error rates for single attempts.

According to 7.2.4.6 the vendor shall test and report security-relevant error rates in accordance with the decision policy of the biometric system. This can mean that multiple attempts may be allowed before a user's transaction is finally considered to be a reject or defensive actions (e.g. blocking an account) may be taken by the biometric system.

While it is obvious that the primary analysis of an error rate should be performed in accordance with the transaction policy, evaluations of different systems become less comparable if they implement different transaction policies. Via this (additional) test of the corresponding error rate for single attempts, the evaluation data should be easier to compare.

For example, if a vendor decides to test and report the FRR in accordance with the transaction policy of the biometric system that allows 3 failed attempts before considering the transaction to be failed, the FNMR (that is the corresponding single attempt error rate) shall be tested and reported as well. Please refer to ISO/IEC 19795-1:2006 for more detailed information about the relationship between the error rates.

NOTE In certain cases it may not be possible to test the corresponding single attempt error rate. Possible reasons may include the design of the biometric system or test policies defined by a concrete evaluation scheme. In these cases the vendor will have to justify why it is not possible to test the corresponding error rate.

7.2.4.8 Statistic approach/confidence values

The vendor shall report the statistical approach which has been used to validate the claim of the maximum values for the security-relevant error rates.

Details of the statistical approach, the confidence level and evaluation results shall be reported by the vendor.

The evaluator will verify that the statistical approach taken is correct and appropriate to validate the claim.

The vendor shall report the confidence level associated with the reported error rates and the evaluator shall check that the confidence limits are suitable for the intended use and required assurance level.

For additional guidance on aspects of the statistical approach please refer to ISO/IEC 19795-1:2006.

7.2.5 Independent testing (Step 6)

The concept of this International Standard defines that testing of the security-relevant error rates is primarily performed, documented and reported by the vendor of the biometric system. However the methodology specified by this International Standard requires the evaluator to validate the vendor test results by conducting an independent test.

The evaluator shall perform independent tests to check the results of the vendor.

During the independent test, the evaluator will specifically address the following questions:

1) Are the results of the vendor's test correct?

2) Does an accumulation of false acceptance cases exist for certain users?

3) How do environmental variations bias the test results?

4) How does a variation of the characteristics of the test crew identified by the vendor to influence the security-relevant error rates bias the test results?

Note that some of the questions that require independent testing may go along with questions in the area of vulnerability assessment. For an efficient evaluation process the evaluator should consider combining these testing activities with the independent testing described before.

To validate the results of the vendor test it may be sufficient for the evaluator to repeat a subset of the tests. Subset testing can, among other things, help to verify that the vendor did not bias their test results by choosing a test population favourable to their desired results.

In other cases, the evaluator may decide that it is necessary to plan and conduct a completely separate test.

The independent analysis shall meet the following requirements:

1) The recruitment of the test crew/test data shall be under the sole control of the evaluator.

2) The planning and execution of the test shall be under the sole control of the evaluator.

The evaluator should follow ISO/IEC 19795-1:2006 to plan and perform the test. However for some aspects of the independent test, the evaluator will have to develop a different methodology.

8 Vulnerability assessment

8.1 Introduction

This subclause focuses on the vulnerability assessment specific to biometric systems. It provides guidance for evaluations by identifying typical vulnerabilities that are common to biometric systems and describes the characteristics of a biometric system upon which these potential vulnerabilities are based.

Further aspects of the environment of a biometric system are considered if they are important in the context of a potential vulnerability, and generic guidance is provided for vulnerability assessment.

The information in this clause shall be used as the basis for a vulnerability assessment in the context of this International Standard as outlined in 6.1.

This clause of this International Standard does not:

— Describe the assessment of vulnerabilities that are common to IT systems in general. For example, if biometric data, biometric references or matching decisions are not protected, an attacker may be able to tamper with that data in order to impersonate someone else. Such vulnerabilities are subject to evaluation under the used methodology (e.g. [3]). However, general vulnerabilities associated with the information handled by the biometric system may also have specific aspects that gain relevance in such a system due to the nature of the information. Therefore, 8.3.1.1 of this International Standard describes a generic vulnerability with respect to the information handled by the biometric system.

— Define a concrete methodology for vulnerability assessment or penetration testing. The approach of this part of this International Standard is to provide evaluation guidelines for biometric systems by identifying generic vulnerabilities of and threats against biometric systems. The concrete methodology for a vulnerability assessment depends on the methodology used for evaluation (e.g. [3]) and the concrete biometric modality that is used. As such, it does not fall into the scope of this International Standard.

8.2 Vulnerability assessment

8.2.1 Overview

Vulnerability assessment benefits from a methodical approach. However, it also requires expertise and creative thinking on the part of the evaluator. Evaluators will therefore need to be aware of the threats, vulnerabilities and countermeasures that exist and in some cases are specific to biometric systems. Information on biometric vulnerabilities appears in 8.3 of this International Standard but evaluators should also seek out further information available in the literature, including public domain reports on biometric vulnerabilities appearing in magazines, academic studies and by searching the internet. Additionally evaluators should acquire practical experience with the techniques of biometric vulnerability investigation as described in these reports. This should be regarded as necessary pre-requisite training for evaluators before conducting a vulnerability assessment as part of a biometric security evaluation under this International Standard.

A security evaluation conducted in compliance with this International Standard shall embody a vulnerability assessment that includes all potential vulnerabilities described in 8.3.

For the descriptions of potential vulnerabilities and requirements, these subclauses refer to biometric subsystems and processes as described in Annex A of this International Standard.

In the context of this International Standard, it is recommended that the security of a biometric system in regards to its potential vulnerabilities is assessed in two consecutive steps:

In **Step 1** the evaluator should examine the system description and seek to identify potential points of vulnerability based on information given in this International Standard, the evaluator's own expertise and other sources such as publicly available reports on biometric vulnerabilities and vulnerability assessments. Using information supplied by the vendor on the vendor assessment of vulnerabilities and countermeasures implemented by the system (including its assumed operational environment), the evaluator will determine whether all potential vulnerabilities have been effectively addressed by technical, procedural and environmental countermeasures. The required level of effectiveness of the countermeasures is determined by the level of assurance required for the evaluation. Details of assurance levels and effectiveness requirements must be defined by the evaluation scheme and are not covered by this International Standard.

The evaluator examines the information provided and determines whether the potential vulnerability is present. If the evaluator cannot refute the existence of the potential vulnerability, it should be considered during further analysis in step 2.

In **Step 2** – after all potential vulnerabilities have been assessed – it is recommended to develop a threat model for the biometric system under evaluation. This threat model considers the results from step 1, the relationship between all vulnerabilities of the biometric system, the generic threats as defined in 8.2.2 and the environment of the biometric system. It should be noted that vulnerabilities cannot be regarded in a fashion which isolates them from one another. It is possible, quite likely even, that a successful threat against a biometric system comprises exploiting multiple vulnerabilities in combination. The threat model should consider all biometric processes of the biometric system including enrolment and de-enrolment.

8.2.2 Biometric system threat overview

Threats against biometric systems can manifest themselves in various ways but are principally aimed at achieving one or more of the following objectives:

— **Impersonation**: A threat against a verification or identification system that is working with a positive claim where an attacker is recognized as another user that is correctly registered, thereby allowing the attacker to obtain the other user's ID.

— **Disguise**: A threat to a verification or identification system that an enrolled user might deliberately change or conceal their biometric characteristic(s) in order to avoid being recognized. This could be a particular threat to a system whose objectives include the prevention of multiple enrolments by a single individual using different identities.

— **Denial of service:** A threat to a verification system or identification system that is working with a positive claim where an attacker repeatedly causes a false rejection, which may cause a biometric system breakdown. This could be a precursor to an attack on a fallback system that is easier to exploit than the disabled biometric system.

The principal threats described above may be manifested in attacks using various techniques against different processes and components used by the biometric system. For example, an attacker could impersonate another person by falsely enrolling as that person, by presenting an artefact containing a copy of the victim's biometric characteristics or by manipulating the enrolment database to replace the victim's biometric reference with that of the impersonator.

Threats are usually taken to be deliberate attempts by an attacker to subvert system functionality. However, it should be noted that, in certain situations, inadvertent actions by legitimate users (including users and operators/administrators) can also lead to the subversion of system functionality.

An example of unintentional impersonation is that of a facial recognition system working in identification mode in which identical twins are enrolled and where it falsely identifies one twin as the other. Note that if the system worked in verification mode this error could not occur without a false claim of identity, which would no longer be regarded as unintentional.

It should be noted that this list of generic threats should be seen as a basis during the development of a threat model and cannot be considered exhaustive or universally applicable.

8.2.3 Additional vulnerabilities

The common vulnerabilities described in 8.3 are potentially applicable to any biometric system. Details will vary with the modality and technology employed and new modalities and technologies may give rise to new variations in the detail. Evaluators will need to interpret the general information given in 8.3 in the context of the modality and technology used in the biometric system under evaluation.

The list of common vulnerabilities described in 8.3 should be regarded as neither comprehensive nor exhaustive. Evaluators will need to study the functionality of the biometric system under evaluation together with its modality and technology. From this evaluators should develop a catalogue of potential threats and vulnerabilities which should be used to provide an agenda for the vulnerability assessment.

The evaluator shall conduct a thorough search for vulnerabilities taking into account the functionality, technology, environment and processes embodied in the biometric system. The search shall not be limited to the vulnerabilities listed in 8.3 of this International Standard.

To determine the rigour and resources that should be applied to the vulnerability assessment, evaluators should follow the guidance given by the scheme under which the evaluation is being conducted.

8.3 Common vulnerabilities of biometric systems

8.3.1 Introduction

The following subclauses identify and explain typical vulnerabilities common to biometric systems.

8.3.2 Performance limitations

8.3.2.1 Overview

One inherent characteristic of biometric recognition is that it is not a wholly deterministic process but is subject to errors that can be expressed in terms of statistical error rates similar to the human factors involved in non-biometric security systems – false accept and reject rates, for example. These and other performance parameters also have implications regarding the level of security provided by a biometric system.

While Clause 7 of this International Standard and ISO/IEC 19795-1:2006 deal with the requirements and principles involved in testing security-relevant error rates, the very existence of those error rates represents an inherent vulnerability of every biometric system.

8.3.2.2 Assessment

In the context of vulnerability assessment, the evaluator should consider the likelihood of an attacker to circumvent the biometric system with a zero-effort impostor attempt.

There are two principal factors in this context.

— The likelihood of a casual attack. This likelihood is determined by factors including the motivation of an attacker, the environment of the biometric system and consequences for a detected attack.

— The chance of a casual attack being successful. This might be quantified in terms of the FAR, so if the FAR is 1 in 10 000, the probability of a casual attack being successful could be quantified as 0,01 %

The two factors will not generally be independent. If a system is known or believed to be susceptible to (successful) casual attacks the likelihood factor will probably increase. Conversely if the system is known or believed to be resistant to (successful) casual attacks, this will probably reduce the likelihood factor.

The evaluation of this potential vulnerability focuses on the following considerations:

— The significance of the remaining risk of a zero-effort impostor attempt based on the results of the tests outlined in Clause 7 and the aspects described before.

— Whether this risk is acceptable for the intended use of the biometric system under evaluation.

It should be noted that – in contrast to other common vulnerabilities – it is very unlikely to have a biometric system that is completely invulnerable to zero-effort impostor attempts. Therefore, the analysis should focus on the question of whether the remaining risk of those attempts is acceptable in the context of the intended use or whether additional mechanisms designed to deter those attempts should be provided by the environment of the biometric system.

8.3.3 Artefact of biometric characteristics

8.3.3.1 Overview

In the context of a biometric system, an artefact is defined as an inanimate object carrying a copy of a human or human-like biometric characteristic(s) made to present to a biometric sensor with aim of spoofing the biometric system into accepting it as the biometric characteristic(s) of a human subject. Examples of biometric artefacts include: prosthetic fingers created out of latex, a photo of a face or a recorded voice. Also a severed human finger (or any severed body part) is regarded as an artefact in the context of this subclause.

Unlike other technical identification and authentication devices, such as smartcards, that have been designed to be difficult to copy, biometric characteristics, which are natural human biological or behavioural properties, have no intrinsic copy protection. It is therefore normally possible to produce a copy of a biometric characteristic in the form of an artefact.

The characteristic carried by an artefact is typically a copy of the biometric characteristic of a human subject, but it is not limited to this case. An artefact could be constructed that contained a synthesised pattern that does not correspond to the biometric characteristic of a particular person or even of any real person. However, the most critical point in the assessment of this potential vulnerability is whether the biometric system will accept an artefact as a valid biometric characteristic.

8.3.3.2 Assessment

Two important issues for a vulnerability assessment are:

— Will the system accept an artefact?

— Will the system process the characteristics of the artefact as human biometric characteristics?

The distinction between the two cases is significant because an artefact is not limited to carrying a copy of a human biometric characteristic; it could carry any synthesised pattern. A biometric system that will accept a realistic biometric characteristic from an artefact might reject a synthesised pattern presented on an artefact because it is not sufficiently human-like.

Evaluators should attempt to distinguish between the two cases by initially using realistic copies with human characteristics, and if these are accepted move on to the case of synthesised characteristics (see 8.3.8 for further details).

The evaluation of this potential vulnerability shall focus on the following questions:

— Whether it is possible to create an artefact of the biometric characteristic being aware of only publicly available information or whether sensitive information will be required.

— How much effort creating an artefact entails.

— Whether the biometric system provides technical countermeasures for the detection and rejection of artefacts, and how effective the countermeasures are in the biometric system under evaluation.

— Whether the technical countermeasures for the detection and rejection of artefacts have any known limitations with respect to their technical specification or operational conditions that can be exploited by an attacker.

The vendor of the biometric system shall provide sufficient information of the mechanisms for artefact detection and rejection to the evaluator.

NOTE 1 The information on artefact detection and rejection may be confidential and represents the IP of the vendor. As such it is very important that this detailed information shall only be provided to the evaluator and not to any customer. This also acknowledges that the evaluator is a trustworthy party due to their independence of the customer and the vendor.

NOTE 2 In the event that a body part severed from a user may be a possible artefact, it should be evaluated how long a severed part can be used with the biometric system. The claim may be made from a medical perspective. No experimental testing may be possible for this case.

The importance of having effective countermeasures against artefacts is related to the difficulty of fabricating a successful artefact, and the difficulty of acquiring a copy of the target human characteristics (assuming that this is the attacker's intention). Some characteristics (e.g. retinal pattern or other vessel pattern) will be hard to acquire directly from the target; others (e.g. face image) may be easy.

Also consideration needs to be given to the possibility that a target's biometric characteristics may be acquired by other means such as from an insecure database containing acquired biometric samples. These factors shall be considered as part of an overall risk analysis in order to determine how effective artefact countermeasures need to be for a particular system.

Some or all of these factors may not be known at the time of the evaluation and it is therefore recommended that for evaluations conducted in conformance with this International Standard, all such factors are ignored. The evaluation of the effectiveness of artefact countermeasures should be performed and reported independently of external considerations. The system risk modelling and assessment process (not defined in this International Standard) will be used to determine whether the results of the artefact countermeasure effectiveness assessment are acceptable in the context of the system use.

8.3.4 Modification of biometric characteristics

8.3.4.1 Overview

Users of a biometric system may intentionally change their biometric characteristics or the presentation of the characteristics in an attempt to avoid recognition or to impersonate an enrolee. Such biometric characteristics can be of behavioural or biological nature. Biometric characteristics and the corresponding samples can change for a number of reasons. For behavioural biometrics such as voice and dynamic signature, users can intentionally modify their normal behaviour. An example of biological biometric characteristics is that of fingerprints where a user could intentionally change the presentation of their finger to the capture device in order to alter the captured sample. This can be done by users to disguise themselves to avoid recognition, rather than to impersonate others. However, impersonation of another user's biological biometrics (facial biometrics, for instance) is also possible, to a certain degree, through the use of make-up or cosmetic surgery. These attacks do not require the use of an artefact and cannot be countered by techniques designed to counter artefacts.

8.3.4.2 Assessment

The critical point of the evaluation of this potential vulnerability is whether the biometric characteristics themselves or captured biometric samples can be intentionally modified by a user in a way that the system is unable to recognize him or her. This would lead to a threat of disguise or denial of service.

The other critical question is whether the biometric characteristics themselves or captured biometric sample can be intentionally modified so that the system falsely recognizes the user as another user. This would lead to a threat of impersonation.

The evaluation of this potential vulnerability shall focus on the question of whether it is possible for an attacker to modify their biometric characteristic in a way that it may be accepted by the biometric system and how much effort and which kind of information would be necessary for such an attack. Furthermore in cases where this may be the aim of an attacker, attention should be paid to the fact that an attacker who has previously enrolled in the system may try to modify their biometric characteristic(s) in order to avoid being recognized (e.g. in a system which has as one of its objectives the prevention of multiple enrolments by a single individual).

To determine the sensitivity of the security relevant error rates to user induced changes in their biometric characteristics or presentation, evaluators shall conduct a representative test of the effect on error rate caused by these changes. The allowed changes to biometric characteristics and presentation shall be defined and controlled for the test. They should be sufficient to demonstrate the effect on error rates but not so large that the system simply fails to work at all It may not be necessary to use the full test crew (that for the Clause 7 performance tests). A small sample of test users will normally be sufficient to reveal the effect of user induced changes on system performance.

For static biometric characteristics such as fingerprints, monitoring the use of the biometric system may be an operational countermeasure against this vulnerability. It should be noted, however, that this countermeasure may not be effective for behavioural biometric characteristics, as the monitoring staff may not be able to determine whether the user has intentionally changed his or her biometric data.

It should be noted that there may be a relationship of this vulnerability to the vulnerability as described in 8.3.5 (“Difficulty of concealing biometric characteristics”). This is specifically true if an attacker is trying to get recognized as another user and needs knowledge about the biometric characteristic of this user in order to convert their own biometric characteristic.

8.3.5 Difficulty of concealing biometric characteristics

8.3.5.1 Overview

It is difficult for a user to intentionally conceal biometric characteristics in their daily life. This type of potential vulnerability depends on the nature of the biometric characteristics used by the biometric system rather than the biometric system functions or the environment of the biometric system.

This potential vulnerability does not include leaks of biometric data from the biometric system (see 8.3.11 for more information on this case). Even if countermeasures against leakage of biometric data in systems are strong enough, attackers may acquire a legitimate user’s biometric sample directly from the user. For example, it might be possible for attackers to obtain a fingerprint that has been left on the biometric capture device, a glass, a table etc. Additionally, faces or voice can be recorded by attackers with a camera or microphone.

The observed biometric characteristics can become the basis to create an artefact or become a target object to convert the biometric characteristic of the attacker (refer to 8.3.3 and 8.3.4 for more information).

8.3.5.2 Assessment

The critical point during evaluation of this potential vulnerability is how difficult it is for the attacker to obtain the user's biometric data in daily life. For example, if there is a trace of biometric data from somewhere (e.g., on a fingerprint sensor), it is easier for an attacker to obtain the data than it would be to directly attain it from the user. It is also easier to obtain biometric data by using a tool (e.g., camera, microphone, etc.) that is publicly available than using a dedicated capturing device.

The evaluation of this potential vulnerability shall focus on the question of whether it is possible to observe the biometric characteristic of a user in their daily life in a way that would allow abuse (e.g. by creating a fake) and how difficult this is.

A special aspect of this vulnerability is the question of whether biometric data remains on the capture device of the biometric system after use and whether this residual data can be abused.

Though the fact that it may be hard in daily life to conceal a biometric characteristic is treated as a vulnerability in the context of this International Standard it should be noted that it is likely that a biometric system cannot do anything against such a vulnerability. If this vulnerability is present for the used biometric characteristic it therefore falls into the scope of a vulnerability assessment to decide whether the risk associated with this vulnerability is acceptable or not – also in the context of other vulnerabilities of the biometric system.

It should be noted that this vulnerability has a strong relationship to the vulnerabilities described in 8.3.3 (“Artefact of biometric characteristic") and 8.3.4 (“Modification of biometric characteristics”).

8.3.6 Similarity due to blood relationship

8.3.6.1 Overview

There is a potential vulnerability in a natural similarity of biometric characteristics between blood relatives. It may lead to a threat that allows one such individual to impersonate a relative. An obvious case is that of identical twins and biometric systems using specific modalities such as face and DNA. In other cases, and more generally, there may be a statistically significant closer similarity of certain biometric characteristics between blood relatives than that found between unrelated individuals. Such similarities could result in a statistically higher than normal False Match Rate between blood relatives than that for randomly selected populations.

This type of potential vulnerability does not include a natural similarity where some biometric data between users without any blood relationship is incidentally similar. This type of similarity falls into the context of the performance of the biometric system as outlined in Clause 7.

8.3.6.2 Assessment

The evaluation of this potential vulnerability shall focus on the questions:

— What is the effect of such similarities on the security related error rates?

— Whether the security-relevant error rates are higher among blood relatives than for other users.

NOTE It should be noted that the assessment of this potential vulnerability does not necessarily have to focus on the scientific questions of how similar each set of biometric characteristics from users who are blood relatives are by nature. The critical point of the evaluation is whether the biometric data that is used by the system is more similar for blood relatives than for other users.

One of the tests that measure the similarities of the biometric characteristics of blood relatives could be seen as an assessment of the security-relevant error rates under special conditions. In such a test, relevant error rates calculated for a test crew consisting of members with no blood relation are compared to the corresponding error rates calculated for a test crew of blood relatives.

This accuracy assessment should follow the same principles as the test for security-relevant error rates as described in Clause 7. However, it should be noted that it may be very hard to obtain a sufficient number of samples from blood relatives to meet all statistic criteria of such a test. In such cases, the evaluator can consider information on the biological background of the biometric characteristic and the characteristics of the Feature Extraction component of the biometric system to obtain sufficient assurance.

Cases where natural similarity of the biometric characteristics of blood relatives poses a threat to the security of a biometric system will need to be addressed in the overall risk management strategy. This is outside the scope of this International Standard.

8.3.7 Special biometric characteristics

8.3.7.1 Overview

Biometric systems are usually designed to provide the maximum degree of distinction between different enrolees, while minimising the degree of distinction between different samples captured from the same enrolee. However for each system there may be individuals with special biometric characteristics that fall outside the design range of normality for the system and which consequently yield substantially higher error rates than normal.

Special biometric characteristics may give rise to vulnerability if they result in higher error rates than those measured by the normal statistical performance testing of Clause 7. Note that such special biometric characteristics do not have to be the result of any deliberate modification of the characteristics as described in 8.3.4.

Users displaying higher or lower error rates than normal for a biometric system are sometimes referred to as “goats”, “lambs” or “wolves”, depending on the error rate affected and the direction of the effect. Although these labels are attached to the subjects, it is important to realise that the effect is a function of the interaction between the user and the system. A user who is classed as a “wolf” in one biometric system will probably not be a wolf in another system using the same modality but implemented with different technology.

8.3.7.2 Assessment

This potential vulnerability can be investigated by examining the results of the performance test described in Clause 7 to determine, for each security relevant error, whether there are certain users whose error rates significantly exceed the normal for the test crew as a whole.

If this vulnerability is discovered during evaluation, it shall be reported. Prospective system implementers and owners will need to determine, as part of an overall system risk analysis, to what degree this might be a realistic threat. One consideration is how feasible it would be for an attacker to gain the necessary knowledge about the existence of the vulnerability and to be able to exploit it.

Operational auditing processes could be a countermeasure against this vulnerability. For example offline checks on the enrolment database to find vulnerable enrolees (those with near matches to other enrolees who could be targets for impersonation) or online checks on near matches (i.e. cases of near match from different individuals as distinct from FRR for same individual). This is particularly important in the case of biometric identification systems where there is no claim of identity needed.

8.3.8 Synthesised wolf biometric samples

8.3.8.1 Overview

If a biometric system produces unusually high error rates when presented with certain abnormal biometric characteristics this may give rise to a vulnerability. Examples of abnormal characteristics could include those with unusually large or small numbers of features. Such characteristics may not be representative of any human biometric characteristic but could be synthesised and copied to an artefact. Alternatively a synthesised characteristic could be injected electrically during a replay attack or planted in the reference database. Such a characteristic might serve as a biometric “skeleton key” by producing apparent matches against a wide range of normal enrolees or impostors.

The form of such synthesised wolf biometric samples will depend on the modality and technology employed. Typical examples might include:

— feature sets containing abnormally large or small numbers of features, e.g. fingerprint minutiae

— feature sets comprising amalgamations of biometric features from 2 or more individuals, e.g. morphed facial images

Countermeasures could include:

— At the image quality control stage, detection of abnormally large or small feature sets.

— At the comparison stage, scoring that accounts properly for both similarities and dissimilarities between the probe sample and reference feature sets.

8.3.8.2 Assessment

The evaluation should seek to establish whether synthesised biometric characteristics with abnormal features are accepted by the biometric system and can result in incidences of false matches to normal enrolee references.

The evaluator should assess this potential vulnerability in a methodical way. Firstly, a direct investigation of the biometric algorithms should be undertaken to determine if they will accept and process abnormal inputs. This could be done by implanting synthesised abnormal data in appropriate places in the database and allowing the data to be processed (input and comparison) in order to observe whether the test data is accepted by the quality control algorithm and successfully scored against test references by the comparison algorithm. The test data can be synthesised to simulate any specific condition that the evaluator wishes to investigate.

If a vulnerability is found in an algorithm, the evaluator then needs to determine whether this vulnerability could be exploited in an operational system context. Avenues to explore include:

— Potential for the use of synthesised characteristics copied onto artefacts

— Potential for the direct injection of synthesised signals via a replay attack

— Potential for unauthorised modifications to the biometric database

A successful exploitation of synthesised biometric data would therefore likely involve the exploitation of other system vulnerabilities; conversely if these other vulnerabilities do not exist, it would probably not be feasible to exploit the synthesised biometric data vulnerability.

This example illustrates the importance of a methodical approach to investigating component vulnerabilities and to then extending the assessment to investigate whether component vulnerabilities can be exploited in the wider system context. For further information on related vulnerabilities see 8.3.3 (Artefacts), 8.3.11 (Leakage and unauthorised modification of biometric data), and also the note about evaluation of generic IT vulnerabilities in 8.1 (Introduction).

8.3.9 Hostile environment

8.3.9.1 Overview

Deterioration of the Capture Subsystem, such as stains or flaws on a sensor, may also affect the security-relevant error rates. The security-relevant error rates are usually determined in an environment that the developer assumes or recommends (see a an attacker, the measured security-relevant error rates may not be achieved.

A hostile environment could lead to system vulnerability particularly at the capture stage. Effects could range from an increase in security relevant error rates to cases of overload where excess exposure to light (for optical devices), sound (for acoustic devices), humidity (for fingerprint devices) or other forms of signal noise could result in the enrolment of noisy or even null references that might later be matched to similarly noisy verification samples (see also 8.3.10).

8.3.9.2 Assessment

It will probably be impractical to test for the effect of all combinations of hostile environmental conditions on security relevant error rates. Evaluators should therefore identify likely hostile conditions, e.g. abnormal lighting for imaging technology, acoustic signals for acoustic sensors, etc. and test for those conditions.

NOTE Further information on how environmental conditions may affect security relevant error rates can be found in ISO/IEC 19795-1:2006.

If vulnerabilities caused by hostile environmental conditions are discovered, action to mitigate the effects will need to be implemented in the system context to prevent exploitation. This will usually be to ensure that the environmental conditions are controlled such that they are not hostile.

8.3.10 Procedural vulnerabilities around the enrolment process

8.3.10.1 Overview

There are three cases that involve potential vulnerability during the enrolment process.

— An attacker could try to become enrolled into the biometric system by inappropriate registration and enrolment using false (someone else) or bogus (invented) identity documentation. Such an attack, if successful, would allow the attacker to be recognized by the biometric system as another user in future. An attacker could also try to get enrolled into the biometric system with an artefact to generate a false (someone else) or bogus (invented) biometric reference. A successful attack in this case would allow the attacker to be recognized by the biometric system as another user in future. Poor quality biometric references usually adversely affect security relevant (and other) error rates resulting in higher error rates than predicted by the statistical performance testing described in Clause 7. This will not only reduce the security assurance level of operational verifications or identifications involving poor quality references; if an attacker can identify individuals with poor quality references, they could become targets for impersonation attempts.

8.3.10.2 Assessment

The evaluation of this potential vulnerability shall focus on the three cases corresponding to the previous clause:

— Whether the enrolment process is performed in a suitable environment and that all necessary mechanisms are in place to ensure that users will be enrolled using the correct ID.

— Whether the system has an artefact detection and rejection functionality.

— Whether the system has a quality check function in a Signal Processing component or functionality to predict error rates during the enrolment process.

It is likely that a biometric system will not be able to mitigate this vulnerability completely by technical means. Therefore, evaluators should identify and report what reference quality control measures the vendor claims to implement.

8.3.11 Leakage and alteration of biometric data

8.3.11.1 Overview

Though common IT vulnerabilities do not fall into the scope of this International Standard, the possible leakage and manipulation of security-relevant data such as biometric samples, biometric references, comparison scores, threshold settings etc. is an important vulnerability to be considered during each security evaluation. In addition, it should be mentioned that while possible countermeasures for such vulnerabilities are common to IT systems, the role of the information that is handled by the biometric system is specific to the biometric technology.

Unauthorised leakage and alteration of data is a general threat to IT systems and system security. Biometric and other data in biometric systems is often sensitive and must be protected in a similar way to data in IT systems generally.

8.3.11.2 Assessment

Data in biometric systems that is security relevant/critical includes:

— Biometric references data – compromise could result in bogus enrolments, impersonation etc. loss of data could result in privacy violations, identity theft etc.

— Biometric data samples in transit through the system (e.g. the output signal from the capture device) or stored in the system (e.g. fingerprint and face images) – If these are leaked, they could be used to help construct an artefact or for direct injection in a “capture/replay” type attack.

— Decision thresholds and parameters – alteration could result in false acceptance, false rejection, and lead to impersonation or denial of service.

— Audit data – compromise could result in cover-up of attack attempts, removal of evidence of unauthorised changes of security parameters and operator malpractice.

The security evaluation of protective measures against leakage and alteration of biometric data in biometric systems is not specified in this International Standard. Evaluators should refer to existing IT security evaluation methodologies such as [3] for further information on the subject.

9 Privacy

9.1 Overview

Biometric systems often link the biometric data identifying a user to associated data about the user such as name, address, etc. Furthermore, in some cases the biometric data could reveal personal details of the user such as gender, ethnicity or possibly health information. This might particularly be important where the biometric data is in the form of or linked with an image of the biometric characteristic (e.g. face image, fingerprint image).

Therefore, privacy is an important issue to be considered during each security evaluation of a biometric system.

Privacy issues are often addressed by organisational means. In addition, technical security functions or measures are used. Those technical means (e.g. appropriate access control to personal data including biometric data, encryption, secure deletion, etc.) shall be assessed during a security evaluation of a biometric system.

The protecting mechanisms should be described in relation to the underlying general or specific privacy principles derived from national legislation. The evaluation of privacy aspects should always be checked against the intended implementation and usage of the biometric system.

The list of privacy-relevant data and the nature of their associated protections shall be defined by the vendor during evaluation and provided to the evaluator as an input for the following criteria.

The vendor shall provide a complete inventory of privacy related data stored and processed by the biometric system and a description of associated protective measures prior to the evaluation.

The evaluator shall ensure that the defined privacy-relevant data are adequately protected and not used wrongfully.