ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"
Convenorship: **UNE**
Convenor: **Bañón Miguel Mr**

CEN/TC 224/WG 18 European requirements for biometric products Part 1 WD

Document type	Related content	Document date	Expected action
Project / Other		2024-03-27	**INFO**

Replaces: N 2592 CEN/TC 224/WG 18 European requirements for biometric products Part 1 WD

CEN/TC 224/WG 18 "Biometrics"
WG Secretariat: **AFNOR**
Convenor: **Gacon Pierre M.**

TS ERBP-1 WD7

Document type	Related content	Document date	Expected action
Meeting / Document for discussion	Meeting: Berlin (Germany) 5 Jun 2024 Project: 00224277 - -	2024-03-22	**COMMENT/REPLY** by 2024-05-21

CEN/TC XXX

Date: 20XX -XX

(ERBP-1 – **WD7**) **prEN XXXXX: XXXX**

Secretariat: XXX

Personal identification — European requirements for biometric products — Part 1: General requirements and application profile definition

Einführendes Element — Haupt-Element — Ergänzendes Element

Élément introductif — Élément central — Élément complémentaire

ICS:

CCMC will prepare and attach the official title page.

Contents

Page

European foreword

This document (prEN XXXX:XXXX) has been prepared by Technical Committee CEN/TC XXX "Title", the secretariat of which is held by XXX.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For relationship with EU Directive(s), see informative Annex ZA, which is an integral part of this document.

[NOTE to the drafter: Add information about related documents or other parts in a series as necessary. A list of all parts in a series can be found on the CEN website.]

Introduction

The use of remote services has increased significantly. This was boosted during 2020-2021, when many service providers and Administrations migrated most of their processes to online handling. We can find nowadays many online services, such as opening of a bank account, claiming expenses, paying taxes, starting legal actions, etc.

For all these services there is the need of identifying the persons claiming for that service, and doing it in a comfortable, universal, reliable and auditable way. Even though some of those services, in some countries, were deployed using PKIs (Public Key Infrastructures), as recommended by eIDAS, this approach was far away from being used by a significant part of the population.

This situation led to creating identification services using videoconferencing tools, such as using any device camera to scan a document, and capture your face for biometric recognition. This is deployed in many countries and sectors, but using ad-hoc solutions, limiting interoperability and increasing costs and risks.

In this context, service providers and Administrations have to define their own requirements, select the products and deploy the solution. On the other hand, manufacturers had to implement different solutions to different customers, in order to fulfil each of those requirement sets. Both sides would benefit from standards and regulations, on which to rely for the product definition.

Everybody will benefit from having a common way of defining those requirements, and a detailed evaluation methodology. These two items can be used by conformity assessment bodies or by business owners, to create their own certification schemes for this kind of technology/products, by following the international ISO/IEC 17000 series of standards.

This Technical Specification is addressing this need for the case of Biometric Products, analysing and merging all current works, and defining a detailed set of requirements, a biometric-mode-specific evaluation methodology, and the passing criteria for different application profiles. This work is developed in accordance with GDPR principles.

The specifications given in this document are based on ISO/IEC 15408-1, ISO/IEC 19989-3 and the ISO/IEC 17000 family of standards, including ISO/IEC 17007, ISO/IEC 17025 and ISO/IEC 17065. These standards are the ones defining all processes dealing with evaluation and certification of products and services, either related to their functionality or to their security.

These objectives are reached by the development of a multipart Technical Specification with the following structure:

— Parts 1-3: Defining the generic principles and methodologies, not requiring a biometric mode specific approach. In particular these parts will be:

  — Part 1: General requirements and application profile definition
  — Part 2: Interoperability tests
  — Part 3: Functionality evaluation methodology

— Parts 4-n: Defining the particularities of each biometric mode (e.g., specific tests, specific requirements), and containing, each of the parts, a set of application profiles, that will establish the test and requirements applicable for a specific application and context. Those application profiles will be written as individual annexes, following the structure provided in Part 1. The numbering of these parts, has been done trying to keep conformance with the numbering used by ISO/IEC 19794 series of standards (WG3). Therefore:

  — Part 4: Fingerprint biometrics
  — Part 5: Face biometrics

— Etc.

1 Scope

This TS series provide a generic framework for the establishment of requirements and their evaluation methodology for biometric products. The requirements will be established depending on the biometric mode considered, and they will be adapted to each scenario, through the definition of a variety of application profiles. In addition, this TS series provides the definition of the individual tests that can be applied to a biometric product.

This document specifies the context for the evaluation of biometric products within the context of the European Union, as well as the general requirements for such evaluation. This will be defined in a biometric mode-independent point of view, as well as not being biased by the particular application which is the target of the biometric product to be assessed.

This first part defines the following items:

— The actors involved in the conformity assessment of biometric products

— Biometric evaluation process

— Biometric evaluation phases

— How to define each particular biometric test

— How to define the profiling for a particular application

NOTE Additional parts are provided covering the specifics of each biometric mode. For each of these modalities, application-independent tests are defined, as well as a set of application profiles, that detail the applicable tests, the evaluation parameters, and the passing criteria.

The Technical Specifications within this series can be taken by any certification body and/or sector, to define and evaluate the requirements for their biometric products within their selected applications. This may be used in coordination with other current National initiatives. For governmental applications, the relevant Government will decide if this evaluation is applicable or not.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 17007, *Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment*

ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*

ISO/IEC 19989-1, *Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework*

ISO/IEC 19989-3, *Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection*

ISO/IEC 30107-1, *Information technology — Biometric presentation attack detection — Part 1: Framework*

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

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
Conformity Assessment Body
CAB
organization that performs conformity assessment operations, such as calibration, testing, certification and inspection.

Note 1 to entry: A Conformity Assessment Body (CAB) may be either the certification body, a testing laboratory, or both.

3.2
evaluation scheme
rules, procedures and management to carrying evaluations of IT product security

Note 1 to entry: An evaluation scheme implements all parts of the ISO/IEC 15408 series.

3.3
evaluation technical report
ETR
documentation of the overall result of the evaluation and its justification, produced by the Testing Laboratory (TL), and submitted to a Certification Body (CB)

3.4
evaluator
individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology

Note 1 to entry: An example of evaluation standards is the ISO/IEC 15408 series with the associated evaluation methodology given in ISO/IEC 18045.

[SOURCE: ISO/IEC 19896-1:2018, 3.5]

3.5
product manufacturer
PM
organization responsible for the development of the target of evaluation (TOE)

3.6
Security Target
ST
implementation-dependent statement of security requirements for a target of evaluation (TOE) based on a security problem definition

3.7
Target Of Evaluation
TOE
set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

3.8
user
human, technical system or one of its components interacting with the target of evaluation (TOE) from outside of the TOE boundary

4 Acronyms and abbreviated terms

CAB Conformity Assessment Body

CB Certification Body

CSA Cybersecurity Act (Comission, n.d.)

eIDAS electronic Identification, Authentication and Trust Services

eIDAS2 new version of eIDAS

ETR Evaluation Technical Report

EU European Union / European

GDPR	General Data Protection Regulation
ID	Identity
LoA	Level of Assurance
PAD	Presentation Attack Detection (as described in ISO/IEC 30107-1)
PM	Product Manufacturer
ST	Security Target
TL	Testing Laboratory
TOE	Target of Evaluation
TSFI	TOE Security Function Interfaces

5 General concepts

5.1 Evaluation actors

5.1.1 General

The following actors play an important role within the evaluation of a biometric product:

- Certification Scheme . This is **out of the scope** of this Technical Specification. The certification scheme is provided by a third party (i.e., Scheme Owner) that, based on the specifications, requirements and methods defined in standards like this one, provide the rules for certifying relevant products and/or services.
- Conformity Assessment Body (CAB)
    - CAB Certification Body (CB) – which is outside of the scope of this document
    - CAB Testing Laboratory (TL)
- Sponsor
- Vendor
- Product Manufacturer (PM)
- User

Each of those actors are described in following subclauses.

The relationship between some of these actors is summarized in the following figure:

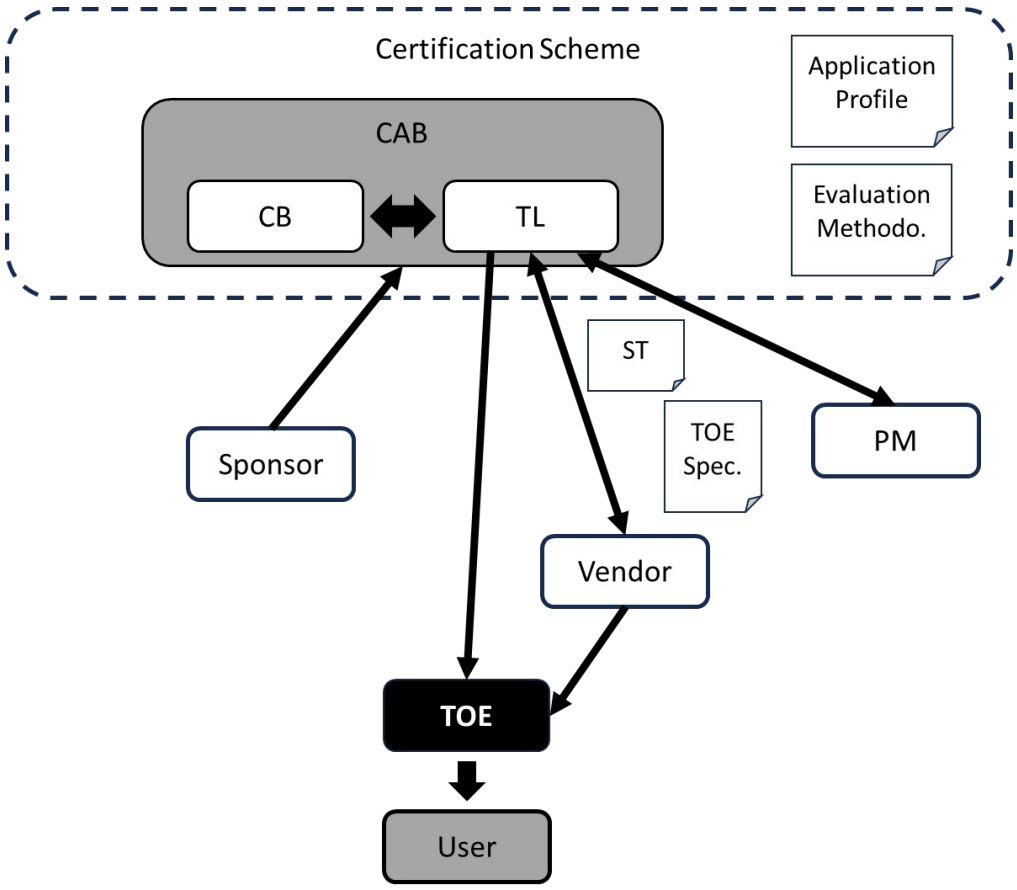

Figure 1 - Relationships among the elements involved in the evaluation

The sponsor will request the evaluation to the CAB, including which is the Application Profile that will be applicable to the TOE. Then the PM or the Vendor will provide the TL with the relevant documents needed to start the evaluation (i.e., the ST and the TOE Specification). Then the TL will plan and execute the relevant tests according to the Application Profile and the Evaluation Methodology, to the TOE. If the TOE passes all the evaluation, then the User may use the TOE, provided typically from the Vendor.

Within the scheme, the following is defined:

- Policies – out of scope of this document
- Biometric Evaluation Methodologies (Part 2 and 3 and individual tests in parts 4-x)
- Biometric Application Profiles (annexes in each part 4-x)

EXAMPLE Examples of policies are a) the requirement for TLs to be ISO/IEC 17025 certified, and/or b) how is the certificate and its duration issued, etc.

5.1.2 Conformity assessment bodies (CAB)

5.1.2.1 Certification body (CB)

A certification body is an accredited independent third party that handles a certification process. Certification bodies are impartial third parties independent of the target of certification, and they shall have the competence specified in international standards and other prerequisites for their operations.

The certification body assesses whether the system, product or person complies with the certification requirements.

Its role consists in:

— Preparing the certification

— Issuing the certificate

— Accrediting the testing laboratory

The certification is valid for a fixed period, after which time a recertification can be performed. The maintenance of the certification may include assessment procedures to be performed during the validity of the certification. The periodicity of the certificate validity shall be defined in the certification scheme, which is not in the scope of this standard series.

The certification body shall comply with the requirements provided by ISO/IEC 17065.

5.1.2.2 Testing Laboratory (TL)

The testing laboratory is a third-party conformity assessment body that performs one or more of the following activities:

— calibration

— testing

— sampling, associated with subsequent calibration or testing [adopted from ISO/IEC 17025].

The role of the testing laboratory is to apply the testing methodology described in the parts 2 to N (depending of the TOE). The detailed specification of the tests to be performed and its methodology is given in the corresponding application profile applicable to the TOE (see clauses 5.2, 5.2.2 and 6).

NOTE It is recommended that the Testing Laboratory is able to comply with the requirements provided by ISO/IEC 17025 or equivalent.

Evaluators are the staff in charge of performing the conformity assessment.

The CAB or the TL must employ or be able to call on a sufficient number of staff to cover the operations related to the evaluation, as well as the applicable standards and other normative documents.

Evaluators shall have the skills appropriate to the functions they perform, including the ability to make the necessary technical decisions, define policies and implement them.

NOTE The evaluation may need special equipment as well as in-depth knowledge about biometrics.

As a synthesis, all evaluators shall act impartially, be competent and work in accordance with the CAB management system.

5.1.3 Sponsor

The sponsor is the entity the contacts the CAB in order to request the certification of the TOE. The sponsor can be related to the manufacturing or selling of the TOE, or it can be a third party interested in evaluating the TOE.

5.1.4 Vendor

The vendor is the entity in charge of selling and/or distributing the biometric product (i.e., the TOE). The vendor may be the sponsor and/or the PM.

5.1.5 Product manufacturer (PM)

The product manufacturer (PM) produces the TOE and is responsible for providing the evidence required for the evaluation (e.g. training, design information), on behalf of the sponsor. The PM may be the sponsor of the evaluation.

5.1.6 User

The user is either a human being or a machine, that interacts with the biometric product once the biometric product is sold or deployed. The user is an actor that do not take part in the evaluation, but for whom the evaluation is thought.

5.2 Evaluation process

EDITOR'S NOTE: From a LATE comment received in March 2024, a question was raised so as to consider if in this section there should be a subclause on handling the updates and/or re-evaluation. An alternative is to consider this within the certification schema, which is out of the scope of this document. It is also important that updates are considered in ERBP-3 for ML-based products, which could be extended to non-ML-based products.

5.2.1 Overall description

Before performing the evaluation's tests, the Sponsor or the Product Manufacturer will have to provide two documents:

— Security Target (ST): (see clause 5.3.2), that will help the TL to detect the points where the security evaluation shall focus.

— TOE Specification: which defines the TOE design (i.e., the functional relationships among subsystems and modules) and the information exchange with the external world (TSFIs)

NOTE It may happen that the Sponsor and/or the PM may need the assistance of a third-party consultant, or even the TL selected, to define such documents.

The evaluation process is set on four different phases:

— Phase 1: interoperability (see clause 5.2.2.1)

— Phase 2: functional evaluation (see clause 5.2.2.2)

— Phase 3: functional boundaries testing (see clause 5.2.2.3)

— Phase 4: attack detection testing (see clause 5.2.2.4)

The TL may consider the most appropriate order of carrying out each of the phases, although the expected order is the one shown in Figure 2. By passing Phase 1, the TL can be sure that all the different test in phases 2 to 4 will not present any problem dealing with interoperability. By passing Phase 2, the TL can be sure that

the TOE is able to reach the documented functionality; if the TOE fails in Phase 2, then executing Phases 3 and 4 may be omitted. Phase 3 will help to understand the limits of the TOE, that will serve the TL to better know the TOE and design more accurate tests in Phase 4.

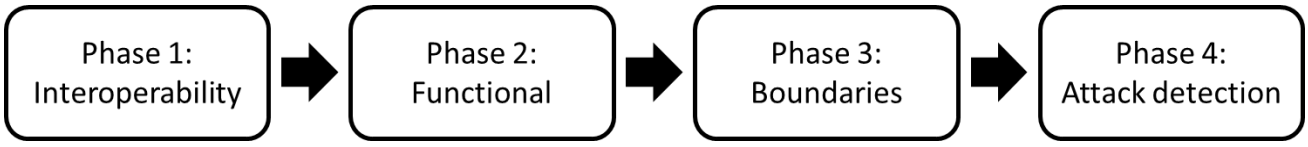

Figure 2 - Expected execution order of the evaluation phases

Depending of the biometric mode used by the TOE, the possible tests performed during each phase are described in the corresponding part of this standard series.

EXAMPLE If the TOE is using face recognition, the different tests performed during each phase are described in the part 5 of this standard series.

For each biometric mode, different parts of this standard series, contain annexes with application profiles (see clause 6). The application profile defines the TOE, as well as the applicable tests to take into account during the TOE assessment for a specific typology of product.

EXAMPLE In the part 5 of this standard series, we can find application profiles for Video-identification using video-conferencing tools or ID wallet application using face recognition for instance.

Eventually, the application profile also determines different level of evaluation with adapted parameters to be compliant with the three levels of assurance (basic, substantial and high) defined in the EU CSA (Comission, n.d.).

Once the evaluation is finished, the TL will issue an Evaluation Technical Report (ETR).

5.2.2 Evaluation phases

5.2.2.1 Phase 1: Interoperability

The main target of this phase is to verify the TOE behaviour regarding what it has been declared by the product supplier. This is to be checked using the relevant settings for the application profile selected.

5.2.2.2 Phase 2: Functional evaluation

The main target of this phase is to evaluate the functional performance of the TOE as to verify that the TOE behaviour corresponds to what it has been declared by the product supplier. This is to be checked using the relevant settings for the application profile selected.

5.2.2.3 Phase 3: Functional boundaries testing

The main target of this phase is to evaluate the TOE to find its functional limits. This will allow to locate the operating boundaries in using the TOE with bona-fide subjects. This knowledge may help evaluators to discover strategies to attack the TOE during Phase 4 tests.

Results obtained will be checked with the TOE documentation, as to check is the failed tests are clearly excluded from the TOE usage

5.2.2.4 Phase 4: Attack-detection evaluation

The main target of Phase 4 is to determine if the TOE is vulnerable to presentation attacks, either of Type 1 or Type 2 attacks (as defined in ISO/IEC 30107-1).

According to the application profile, the evaluated attacks may be impostor attacks, concealer attacks or both.

Under a high-level security conformity assessment, as a general rule, any evaluation attempt resulting in a pass, will declare a failure in Phase 4 for the TOE. This will be determined by analysing that the attack is not exceeding the maximum attack potential for the TOE evaluation.

5.3 Documents involved in the evaluation

5.3.1 Application Profile

This document shall be public and be written either as an Annex to any part of this TS series, or by any independent institution, such as governments, intersectoral associations, etc.

The content of the Application Profile is defined in clause 6.

5.3.2 Security Target (ST)

This document shall be public and be written by the Sponsor, Vendor and/or Product Manufacturer.

At beginning of the assessment, the evaluator needs to read the Security Target declaration of the TOE (ST) provided by the Sponsor and/or PM. This is a document that describes the TOE and the perimeter of the evaluation: the assets protected by the TOE, the threats taken into account during evaluation and the security functions implemented by the developer to prevent the threats. The ST will give information about the TOE to the evaluator and will influence the attack rating if an attack bypasses the TOE (see Clause 5.6.3). The ST shall have the following structure, based on the structure described in ISO/IEC 15408-1 standard:

a) Synthesis
    1) Identification of the product to be evaluated
b) Argument
    1) General description of the product to be evaluated, including the type of biometric product and biometric modalities involved.
    2) Description of the use of the product to be evaluated, with a focus to the use of the biometric functionality and the user interaction.
    3) Description of the intended use environment, in particular, if there is any environmental factor that may impact the performance of the biometric solution.
    4) Description of dependencies
    5) Description of typical users
    6) Description of the TOE
c) Description of the technical operating environment
    1) Assets to be protected by the TOE when using the biometric functionality.
d) Description of threats within the biometric subsystem.
e) Description of the security mechanisms of the TOE, related to the biometric functionality

f) Threats coverage

In addition to this content, the ST shall also include those additional items required by the applicable application profile (see clause 8.6).

Once the evaluator has read and checked the correctness of the ST, the evaluation can begin.

5.3.3 TOE Specification

This information is not intended to be public, but only to be seen by CABs. This information may be split in several documents, such as:

— TOE Design

— TOE Functional Specification

— TOE Architecture

5.3.4 Evaluation Technical Report (ETR)

Consistent reporting of evaluation results facilitates the achievement of the universal principle of repeatability and reproducibility of results. Those results are documenting in the Evaluation Technical Report (ETR).

The TL delivers the ETR to the CB. Requirements for controls on handling the ETR are established by the certification scheme which may include delivery to the sponsor or PM. The ETR may include sensitive or proprietary information and may need to be sanitised before they are given to the sponsor or PM.

This document defines the ETR's minimum content requirement; however, certification schemes may specify additional content and specific presentational and structural requirements. The reader of the ETR is assumed to be familiar with general concepts of the evaluation of biometric products, and in-depth knowledge of the TOE.

The ETR supports the CB to confirm that the evaluation was done following all applicable requirements, but it may happen that additional information may be needed, and required by the CB to the TL.

The minimum content of the ETR is specified in the following list of items:

— Introduction

— Evaluation

— Results of the evaluation

— Conclusions and recommendations

— List of evaluation evidences

— List of acronyms / Glossary of terms

— Observation reports

Each of these items is described in the following subclauses.

5.3.4.1 Introduction

As a general rule, the TL shall report about:

— Evaluation scheme identifiers (e.g. logos), which are the information required to unambiguously identify the scheme responsible for the evaluation oversight.

— The ETR configuration control identifiers, which contain information that identifies the ETR (e.g. name, date and version number).

— The Application Profile configuration control identifiers (e.g. name, date and version number), which are required to identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.

— The identity of the PM.

— The identity of the sponsor, which is required to identify the party responsible for providing evaluation evidence to the TL.

— The identity of the TL and the evaluator, which is required to identify the party performing the evaluation and responsible for the evaluation verdicts.

5.3.4.2 Evaluation

The TL shall report the evaluation methods, techniques, tools and standards used. Also, the TL shall reference the evaluation criteria, methodology and interpretations used to evaluate the TOE under the relevant Application Profile.

The TL shall report any constraints on the evaluation, constraints on the handling of evaluation results and assumptions made during the evaluation that have an impact on the evaluation results.

The TL may include information in relation to legal or statutory aspects, organisation, confidentiality.

5.3.4.3 Results of the evaluation

The TL shall report a verdict and a supporting rationale for each test executed, as a result of performing the corresponding evaluation methodology action.

The rationale justifies the verdict using the relevant parts of this Technical Specification, together with the applicable Application Profile. It will include any interpretations and the evaluation evidence examined and will show how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results.

5.3.4.4 Conclusions and recommendations

The TL shall report the conclusions of the evaluation, in particular the overall verdict as defined in the Application Profile.

The TL may provide recommendations that may be useful for the CB and/or the certification scheme.

5.3.4.5 List of evaluation evidences

The TL shall report for each item of evaluation evidence the following information:

— the issuing body (e.g. the PM, the sponsor);

— the title;

— the unique reference (e.g. issue date and version number).

5.3.4.6 List of acronyms / Glossary of terms

The TL shall report any acronyms or abbreviations used in the ETR.

Glossary definitions already defined in this series of Technical Specifications need not be repeated in the ETR.

5.3.4.7 Observation reports

An observation report is a report written by the TL requesting a clarification or identifying a problem during the evaluation. The TL shall report a complete list that uniquely identifies the observation reports raised during the evaluation and their status.

6 Definition of the levels of assurance (LoA)

EDITOR'S NOTE: This clause has been copied from Kevin's project on Digital Injection Attacks. For the working phase, this will be kept also in here, but later on, it will be deleted, and substituted by a text referencing to Kevin's project and noting the differences. That will avoid duplication of information, and will allow Kevin's project to be published before this one. When the TS on Digital Injection Attacks is published, this clause will be changed with the following text highlighted in Green.

An important aspect within the evaluation methodology defined in this European Standard series, is to associate both the TOE, and the evaluation to be performed (i.e., the Application Profile) with a certain Level of Assurance (LoA), as defined by CSA (Comission, n.d.). In order to determine the LoA, the attack potential shall be calculated in accordance to ISO/IEC 19989-1 and ISO/IEC 19989-3. The application of these international standards to the evaluation or biometric products in Europe, is defined in TS XXXX on Digital Injection Attacks (clause titled "XXXXX"), which is taken in this European Standard series as a basis.

6.1 Introduction

This clause is filled in accordance with ISO/IEC 19989-3. It provides the definition of the different levels of attack potential, as well as the different Levels of Assurance (LoA).

Also, in order to calculate the attack potential, the different parameters and its weights are described.

NOTE These specifications are also included in the TS XXXX on Digital Injection Attacks. They are expected to be identical between both projects.

6.2 Levels of difficulty of the evaluations

EDITOR'S COMMENT: To be updated with the final content of the TS on Digital Injection Attacks.

6.3 Attacks rating methodology

6.3.1 General

Giving a level of difficulty to an attack is really useful as it allows to give an indication of the risks incurred by a product (and its data) equipped with a biometric security. With this biometric attack rating methodology, each evaluation laboratory will be able to give a mark to possible attacks on the TOE.

In this methodology, criteria are associated with marks in order to give a weight to each attack, to attribute then the intended level of attack (basic, substantial or high) in function of this weight. The EU Cybersecurity Act recommends these three assurance levels (basic, substantial or high) to express the cybersecurity risk. These assurance levels are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. This document uses the same vocabulary to correspond to what is currently used in cybersecurity.

Depending on the attack, each criterion gives a rating to the attack, and the sum of all these marks gives a total weight to the attack. Thanks to this weight, the evaluator will give a level to the attack.

Table 1 lists the levels of attack with their weight's intervals.

Table 1 — Attack levels and AVA_VAN levels

Weight interval	Attack's level (resistance)	Highest assurance level met
0 to 9	No rating	-
10 to 19	Basic	AVA_VAN.1
20 to 29	Enhanced Basic	AVA_VAN.2
30 to 39	Moderate/Substantial	AVA_VAN.3
40 and above	High	AVA_VAN.4 or AVA_VAN.5
At least one "Not Practical" mark	Not Practical	

Not practical corresponds to the limit of an evaluation laboratory. The lab can estimate that an attack is not achievable by a random attacker, but only by powerful organizations (e.g., intelligence agencies, terrorist groups, etc.). Thus, if a criterion is associated with a "not practical" mark, the attack will be considered not achievable and will get the level "not practical".

The methodology considers two phases of the attack: identification and preparation.

NOTE This methodology is inspired by the Joint Interpretation Library (JIL) attack rating methodology used for smartcard security evaluations. It has been adapted to biometric systems but is based on the same structure. (European Parliament, 2016)

NOTE 2 The level of an attack can vary through time.

6.3.2 Identification and exploitation phases

The identification phase measures the effort required to create the attack. The advantages given to the laboratory to allow the first implementation of the attack within a reasonable time must be taken into account. These benefits can be of different natures, such as:

- access to non-public information (source code, design documents) or even confidential information (crypto keys, error logs).
- access to a product whose configuration is advantageous for the attacker compared to the operational configuration.

The exploitation phase measures the effort required to reproduce the attack in operational condition. The attacker is supposed to have useful information and automatic tools from the identification phase. On the other hand, the attacker is no longer supposed to have any particular advantages other than the information resulting from the identification phase.

Each criterion will give a weight to the attack for each phase.

The total weight, i.e., the sum of the weights of both phases, is the one to be used to determine the assurance level met (i.e., the AVA_VAN level), by using Table 1.

The different criteria considered by this methodology are described in the next subclauses.

6.3.3 Time effort

The time effort is the time spent by an attacker in order to achieve an attack against a biometric system. The number of days corresponds to “working days”, as this methodology will be applied by TLs.

Table 2 lists the time effort weight’s intervals for identification and exploitation phases.

Table 2 — Time effort weights

Interval	Identification weight	Exploitation weight
< one hour	0	0
< one day	1	3
< three days	2	4
< 7 days	3	6
< 25 days	6	8
> 25 days	10	10
Not practical	*	*

BSI COMMENT: Speaking for the consumer world (smartphones / tablets) typically 3 days 72h are the upper limit to attack the biometric system.

6.3.4 Expertise

BSI COMMENT: Time effort and expertise are somehow linked to each other. I am not sure if these two parts scale in an applicable manner

Expertise levels are defined based on the attacker ability to achieve the attack, on his/her knowledge (software, hardware…) and on his/her ability to operate the necessary tools.

These are the three levels of expertise:

- Laymen
- Proficient
- Experts

Laymen are attackers who have no particular expertise in any field linked to the attack. BSI COMMENT: Maybe adding knowledge from public sources (youtube…) as a trait of the laymen can clarify the difference between the laymen and a proficient.

Skilled attackers are familiar with the security behaviour of the product type and are familiar with laboratory measurements and equipment.

Experts are attackers who has expertise in a field or equipment linked to the attack and necessary to achieve the attack. BSI COMMENT: For me this sentence implies that the ownership of a specialized tool / equipment needed to perform an attack defines someone automatically as an expert.

In very specific cases, several types of expertise are required to make an attack. The "Multiple experts" level can be used but it should be noticed that the different skills must concern fields that have nothing to do with each other, for instance expert in motion design and mobile penetration testing.

Table 3 lists the expertise weight's intervals for identification and exploitation phases.

Table 3 — Expertise weights

Interval	Identification weight	Exploitation weight
Layman	0	0
Skilled	2	2
Expert	5	4
Multiple experts	7	6

6.3.5 Knowledge of the product under evaluation

Knowledge of the product under evaluation refers only to classification levels related to the identification and exploitation of vulnerabilities in the product under evaluation.

In general, it is expected that all knowledge required in the exploitation phase of the attack will be passed on from the identification phase by way of suitable scripts describing the attack. To require sensitive or critical information for exploitation would be unusual.

The classification of the information for this criterion will be determined by the protection of the information. The higher the classification, the more difficult it will be for an attacker to retrieve the information required for an attack.

The following classification for information about the product under evaluation is to be used:

- **Public information:** information is considered public if it can be easily obtained by anyone (from internet for instance) or if it is provided by the developer to any customer without further means.
- **Restricted information:** information is considered restricted if it is controlled within the developer organization and distributed to subcontractors or special customers under a non-disclosure agreement.

- **Sensitive information:** this is knowledge that is only available to discrete teams within the developer organization. Sensitive information is protected by appropriate technical, environmental and organizational means. If such information needs to be distributed to or accessed by other organizations outside the developer, this must be limited to a strict need-to-know basis protected by a specific contract.
- **Critical information:** this is knowledge that is only available to teams on strict need-to-know basis within the developer organization. Critical information is physically and environmentally protected by high secure infrastructure as well as secure physical environment including attack detection and attack prevention layers. If such information needs to be accessed by other organizations than the developer, this must be limited to a strict need-to-know basis protected by a specific contract.

Table 4 lists the knowledge of the TOE weight's intervals for identification and exploitation phases.

Table 4 — Knowledge of the TOE weights

Interval	Identification weight	Exploitation weight
Public information	0	0
Restricted information	2	2
Sensitive information	4	3
Critical information	6	5

BSI COMMENT: "In general, it is expected that all knowledge required in the exploitation phase of the attack will be passed on from the identification phase by way of suitable scripts describing the attack." Therefore, why is it necessary to mention at this point exploitation weights instead of increasing the weights for the identification phase.

6.3.6 Equipment

Equipment refers to the hardware/software or tools that are required to perform the attack on the product under evaluation.

We separate equipment in five different categories:

- Standard equipment: equipment that is affordable and easily available to the attacker. BSI COMMENT: What does affordable mean? Speaking in terms of PAIs (face masks) an attacker does not necessarily own the very expensive equipment, public services may be used to manufacture high sophisticated PAIs.
- Specialized equipment: this refers to fairly expensive equipment and/or not available in standard markets
- Bespoke: this refers to very expensive equipment and/or with difficult and controlled access. In addition, if more than one specialized equipment are required to perform different parts of the attack, this value can be used. EDITOR'S COMMENT: The market availability does not matter for the definition of Bespoke. Adding the definition of being not available in standard markets, whatever standard market means, and the option to customize the equipment.
- Multiple Bespoke: this refers to a situation, where different types of bespoke equipment are required for distinct steps of an attack
- Not Practical: the equipment required to perform the attack is too expensive or too difficult to obtain when compared with the possible gains or advantages which could be seeked by an attacker.

Table 5 lists the equipment weight's intervals for identification and exploitation phases.

Table 5 — Equipment weights

Interval	Identification weight	Exploitation weight
Standard	0	0
Specialized	2	4
Bespoke	4	6
Multiple Bespoke	6	10
Not Practical	*	*

6.3.7 Access to TOE

Access to TOE refers to measuring the difficulty to access the TOE either to prepare the attack or to perform it on the target system.

For the identification phase, elements that should be taken into account include the easiness to buy the same biometric equipment (with and without countermeasures).

For exploitation phase, both technical (such known/unknown tuning) and organizational measures (limited number of tries, etc.) should be taken into account.

The number and the level of equipment requested to build the attack is also taken into account in this factor.

BSI COMMENT: Do not understand this point, because the previous section deals with equipment

This factor is not expressed in terms of time. The levels are as follows.

1. Easy: For identification phase, there is no strong constraint for the attacker to buy the TOE (reasonable price) to prepare its attack. For exploitation phase, there is no limit in the number of tries. BSI COMMENT: If an attacker really wants to overcome the biometric system, then I would consider that the price of the TOE does not matter. Would be an Apple Vision Pro for ~3.5k$ a reasonable price to “break” “IrisID”, even if I have to import it to Europe for 6k$?
2. Moderate: For identification phase, specialized distribution schemes exist (not available to individuals) or the limit in the number of tries is deactivated. For exploitation phase, either a tuning of the attack for the final system is required (unknown parameterization of countermeasures for example) or the limit in the number of tries is deactivated.
3. Difficult: For identification phase, the system is not available except for identified users and access requires compromising of one of the actors or critical countermeasures are deactivated (e.g., virtual camera detection system). For exploitation phase, for example IAIs should be adapted to the (unknown) specific tuning or critical countermeasures are deactivated (e.g., virtual camera detection system),

EDITOR’S NOTE: the last sentence, highlighted in yellow, shall be changed in accordance to that it is written in TS DIA.

Table 6 — Access to TOE weights

Interval	Identification weight	Exploitation weight
Easy	0	0
Moderate	2	2
Difficult	4	4

EDITOR'S NOTE: We have changed the criterion "Sample type" by "Access to the TOE" to better align with ISO 19989-1 Annex F.

6.3.8 Access to biometric characteristics

The access to the biometric characteristic or biometric sample is a key element for the attacker in order to achieve a biometric attack, as this is the biometric characteristic of the target that will permit the attacker to perform the attack. The quality of biometric sourcing will influence the attack's quality. Here are the different levels of access to biometric characteristics:

- Not needed. Access to biometric characteristic is not needed during this attack's phase.
- Easy. Samples of these modalities can be collected without difficulty, even without direct contact with an enrolled data subject (an exploration of the web and the social networks and so forth). Examples are 2D face, signature image, and voice signal.
- Moderate require multiple acquisitions, probably in a controlled way, without the collaboration of an enrolled data subject but probably with a direct contact with them. An example would be to make a social engineering attack to get the biometric sample).
- Difficult. The biometric characteristic is captured with specific equipment which requires full cooperation from the target.

NOTE: The similarity between the attacker and the victim, if needed, shall be taken into account as a difficulty to obtain the biometric source.

Table 7 lists the access-to-the-biometric-characteristic weight intervals for identification and exploitation phases.

Table 7 — Access to the biometric characteristic weights

Interval	Identification weight	Exploitation weight
Not needed	0	0
Easy	0	0
Moderate	4	4
Difficult	8	8

EDITOR'S NOTE: We have changed the criterion "Biometric sourcing" by "Access to the biometric characteristic" to better align with ISO 19989-1 Annex F. We have added a criteria called "not needed" to adapt to all scenarios.

6.3.9 Degree of scrutiny

Degree of scrutiny refers to the one applied during usage the TOE. Here are the different existing levels of scrutiny:

- None: the attacker is not supervised while he achieves an attack.
- Overseen: there is at least a security agent, or an operator trained for fraud detection, who oversees the usage of the TOE. However, the control is done quickly in order to be efficient in time and is done remotely.

- Not practical: The security agent is physically present and close from the attacker and the control is really thorough (e.g., the security agent checks the fingers of the individual before fingerprint recognition). The evaluation laboratory can notice that an attack is "not practical" when the level of security control is high enough to consider that an attacker is not enough confident to perform an attack.

Table 8 lists the degree-of-scrutiny weight intervals for identification and exploitation phases.

Table 8 — Degree of scrutiny weights

Interval	Identification weight	Exploitation weight
None	0	0
Overseen	2	3
Not Practical	*	*

6.3.10 Replicability

EDITOR'S NOTE: Add the final text for the replicability criteria in TS for Digital Injection Attacks. Also, discuss with BIO-iTC the possibility of using negative weights for this criteria (instead of 0, 3, 6, using 0, -3, -6).

7 Definition of individual tests

Part 2 of this standard series, as well as each biometric mode part of this standard series (parts 4 to N) shall describe the individual tests to be performed during the different phases by the testing laboratory.

Each test shall have the following content:

— A general description of the test to be performed

— The settings to take into account for these tests

— The materials to use for these tests

— The trials to perform for these tests

— The attempts to perform for these tests

— The data to be included in the Evaluation Technical Report

For more details on the taxonomy about testing used here, we refer the reader to the part 3 of this standard series.

The settings values, the number of test subjects, the metrics and the decision criteria for each test are described in each application profile.

In the case of Phase 4 tests, also the minimum attack level analysis shall be included. For each attack, some of the criteria specified in clause 6.3 can be pre-determined. The rest of the criteria shall be placed to the minimum value, to allow each application profile to specify the interval in which the relevant TOE is located for such criteria.

8 Definition of application profiles

8.1 Introduction

Application profiles are targeting the evaluation of a specific range of product using biometric recognition. They are defined in the annexes of the according biometric mode part of this standard series.

Application profiles are the baseline for getting a conformity with this standard series. Indeed, a specific product can demand an evaluation process to a testing laboratory to get a conformity with the according standard of this series (depending of the biometric mode used by the TOE) AND a specific application profile AT a certain level of assurance (basic, substantial or high). **The application profiles taken into account by testing laboratories must be one of those present in annex of the according part of this standard series. Otherwise, a testing laboratory can't attest a conformity with this standard series.**

An application profile is composed of the following content:

— The description of the targeted typology of products (TOE description)

— The main guidelines for the three evaluation levels of assurance: basic, substantial and high

— The interoperability requirements

— The functional requirements

— The security requirements

— The targeted parameters for each requirement

The application profile defines the mandatory minimum requirements that shall be considered by the testing laboratory to perform a conformity assessment with this standard series and the specific application profile.

8.2 TOE description

This part of the application profile shall describe as detailed as possible the range of products taken into account. It must contain:

— A general description of the TOE from the biometrics perspective (i.e., enrolment, comparison, PAD, etc.)

— The biometric mode used

— A general usage description of the TOE's biometric functionality

— A general architecture of the TOE's biometric functionality

— The capture devices and the environment for using the TOE, i.e., the target operational environment.

8.3 Levels of assurance

This clause in the application profile shall define the LoAs applicable. In order to determine the LoAs applicable, clause 6 of this document shall be used.

The application profile shall also specify any relevant restriction in the parameters to state the attack potential of each test, when such restriction goes beyond the originally defined in the test. In other words, the application profile may also define, for the relevant TOE, if some of the criteria defined in clause 6.3, shall increase its interval, from the minimum one defined at each of the Phase 4 tests.

NOTE This Technical Specification takes the latest definition in the EU context (in particular, that of eIDAS2) for the definition of only 3 levels of assurance (LoA). The mapping of those three levels in relation to other international-considered levels can be found in (ENISA, 2021).

8.4 Phase 1: Interoperability requirements

If the TOE is requiring interoperability with another system, this interoperability's need shall be described in the application profile. The conformity testing with data interchange format and with data quality (if it exists) shall be specified in this clause of the application profile.

For more details about interoperability requirements, we may refer the reader to the part 2 of this standard series.

8.5 Decision criteria for functional tests (Phases 2 and 3)

8.5.1 General

This part of the application profile will describe the functional requirements of the TOE, i.e., the "bona fide behaviour". This consists in defining which tests from Phase 2 and Phase 3 shall be performed by the testing laboratory.

For each selected test, within the possible list of tests defined earlier in the standard, the application profile shall define the values for each parameter tied to the test (the different variables, thresholds, etc.).

EXAMPLE It may consist in defining the test crew, the number of test errors accepted, the number of non-matches accepted, etc.

Eventually, the application profile shall define the decision criteria for the functional requirements. The decision criteria shall be described with the following structure:

Table 9 — Decision criteria for functional requirements testing

VARIABLE	OPERATION	THRESHOLD	VERDICT
Variable 1	*> or <*	*Threshold 1*	***PASS or FAIL***
Variable 2	*>*	*Threshold 2*	***PASS or FAIL***

Each decision criteria shall be linked to an evaluation level of assurance. Thus, if the application profile intends to reach the three different level of assurance, the decision criteria for each functional tests shall be defined for each level of assurance (in different subclauses in the application profile).

8.5.2 Metrics for functional error classification rates

The error classification rates which may be used during the functional requirements testing are the ones defined in the ISO/IEC 19795-1 standard.

8.5.3 Content of this section

When writing the Application Profile, the following subclauses shall be included:

— Phase 2 parameters and passing criteria

  — Overall requirements: including all common aspects for the Phase 2 tests, and a list of the applicable Phase 2 tests.

  — An individual subclause for each of the required tests to be executed, indicating in them all parameters needed for the evaluation.

— Phase 3 parameters and passing criteria

  — Overall requirements: including all common aspects for the Phase 3 tests, and a list of the applicable Phase 3 tests.

  — An individual subclause for each of the required tests to be executed, indicating in them all parameters needed for the evaluation.

8.6 Phase 4: Decision criteria for security requirements

8.6.1 General

This part of the application profile will describe the security requirements of the TOE, i.e., the attack detection. This consists in defining which tests from Phase 4 shall be performed by the testing laboratory.

As a reminder, the application profile determines the mandatory minimum requirements that shall be tackle by the testing laboratory. The testing laboratory is free to perform additional tests if needed. Indeed, during the establishment of the ST, if a specific security function which is not described in the application profile needs to be assessed, the testing laboratory should perform additional specific tests for this security function.

For each selected test, within the possible list of tests defined earlier in the standard, the application profile shall define the values for each parameter tied to the test (the different variables, thresholds, etc.).

EXAMPLE It may consists in defining the number of PAI, the number of presentations, the level of PAI used, etc.

Eventually, the application profile shall define the decision criteria for the security requirements. The decision criteria shall be described with the following structure:

Table 10 — Decision criteria for security requirements testing

VARIABLE	OPERATION	THRESHOLD	VERDICT
Variable 1	*> or <*	*Threshold 1*	***PASS or FAIL***
Variable 2	*>*	*Threshold 2*	***PASS or FAIL***

Each decision criteria shall be linked to an evaluation level of assurance. Thus, if the application profile intends to reach the three different level of assurance, the decision criteria for each security tests shall be defined for each level of assurance (in different subclauses in the application profile).

For security requirements, the threshold to define the verdict of the attack detection can be defined according to two methodologies, which would be selected and specified in the application profile:

— The threshold can be based on an error classification rate value

— The threshold can be based on the quotation of the attack if the attack has been classified as a vulnerability (the attack has been identified and exploited, i.e., the attack has bypassed the TOE twice).

8.6.2 Metrics for security error classification rate

The error classification rates which may be used during the security requirements testing are the ones defined in the ISO/IEC 30107-3 standard.

8.6.3 Attack rating methodology

The attack rating methodology which may be used during the security requirements testing is the one defined in the Clause 12 of the TS Biometric Data Injection Attack detection.

8.6.4 Content of this section

When writing the Application Profile, the following subclauses shall be included:

— Overall requirements: including all common aspects for the Phase 4 tests, and a list of the applicable Phase 4 tests.

— An individual subclause for each of the required tests to be executed, indicating in them all parameters needed for the evaluation.

8.7 Requirements for the overall decision

At the end of the application profile, the requirements for the overall decision shall be defined according to the decision criteria obtained for both functional requirements testing (with testing phases 1 and 2) and security requirements testing (with testing Phase 4).

The rules for the overall decision shall take into account the obtained verdicts of each test and can be adjusted to the evaluation level of assurance if the application profile intends to apply for different evaluation levels of assurance.

Bibliography

Comission, E. (n.d.). *The EU Cybersecurity Act*. Retrieved 12 13, 2023, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

ENISA. (25 de 05 de 2021). *Cybersecurity Certification: Candidate EUCC Scheme v1.1.1*. Recuperado el 13 de 12 de 2023, de https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

European Parliament. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Retrieved from EUR-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj

WG3, I. J. (s.f.). ISO/IEC 19794 (all parts), Information technology — Biometric data interchange formats.