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

Document type	Related content	Document date	Expected action
Project / Other		2023-09-28	**INFO**

Description

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

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

NP TS_ERBP-1 WD5

Document type	Related content	Document date	Expected action
Meeting / Document for information	Meeting: Courbevoie (France) 13 Dec 2023	2023-09-11	**COMMENT/REPLY** by 2023-11-22

CEN/TC XXX

Date: 20XX -XX

(ERBP-1 – WD5) **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-modality-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 the ISO/IEC 17000 family of standards, including ISO/IEC 17007, ISO/IEC 17025 and ISO/IEC 17065. Such family of standards is the one defining all processes dealing with evaluation and certification of products and services.

DISCLAIMER: As we're in initial WDs some terminology will have to be revisited to be compliant.

EDITOR'S NOTE: This project will be developed following ISO/IEC 17007, and also being as close as possible to ETSI TS 119 461, and with the intention to allow also a conformity assessment valid for a potential Common Criteria Light certification.

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 modality 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 modality (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. Therefore:

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

Identification of patent holders, if any.

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 modality considered, and they will be adapted to each scenario, through the definition of a variety of application profiles.

This series of standards are expected to provide the evaluation methodology, the individual tests, and the application profiles (with their particular requirements).

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 modality-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

— Evaluation process

— Evaluation phases

— Operational risk assessment

— Policies and practices

— How to define the profiling for a particular application

NOTE Additional parts are provided covering the specifics of each biometric modality. 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, government 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. Governments may decide to give a higher preference to other National specifications.

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.

EN XXXX-1:XXXX, *General title of series — Part X: Title of part*

EN XXXXX (all parts), *General title of the series*

[NOTE to the drafter: The Normative references clause is compulsory. If there are no normative references, add the following text below the clause title: "There are no normative references in this document."]

EDITOR'S NOTE: This section will be filled in and debugged once the main text is mature, selecting which documents apply to this document, and which of them shall be here and which shall go into the Bibliography.

EDITOR'S NOTE: These are the documents to be used as the basis for this work:

- ISO/IEC 19989-x
- Common Criteria (ISO 15408) Biometrics Security Community – Collaborative Protection Profile PP-Module for Biometric and Verification
- ETSI TS 119 461
- France: ANSSI "Remote Identity Verification Service Providers: Requirements rule set"
- Spain: ETD/465/2021 + LINCE + STIC 140 F11 + IT-14
- Portugal: Decree-Law No. 126/2021:
    - Regulation from Portuguese supervisory body (eIDAS) about "Identification of physical persons through remote identification procedures using videoconference", https://www.gns.gov.pt/docs/despacho-154-2017-id-videoconferencia.pdf
    - Regulation from Portuguese supervisory body (eIDAS) about "Identification of physical persons through rremote identification procedures using automatic biometric facial recognition systems", https://dre.pt/dre/detalhe/despacho/2705-2021-159088948
- Germany: BSI TR-03121, BSI TR-03122
- BSI Technical Guideline TR-03166 for Biometric Authentication Components in Devices for Authentication
- ISO/IEC 17067
- ISO/IEC TR 17026
- ISO/IEC 17028
- ISO/IEC 17032

EDITOR'S NOTE: Within this WD we will be:

- Fully compliant with 17007 for drafting the document
- Fully compliant with 17065 for CAB reviewer
- Fully compliant with 17025 for CAB evaluator

3 Terms and definitions

EDITOR'S NOTE: To be defined during project drafting

For the purposes of this document, the following terms and definitions apply / the terms and definitions given in… 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

[NOTE to the drafter: The Terms and definitions clause is compulsory. If there are no terms and definitions, add the following text: "No terms and definitions are listed in this document."]

3.1

Conformity Assessment Body

organization that performs conformity assessment operations, such as calibration, testing, certification and inspection.

Note 1 to entry: A CAB designates both the certification body and the testing laboratory.

3.2

term

text of the definition

Note 1 to entry:

[SOURCE: EN XXX:XXXX, definition XX]

4 Acronyms and abbreviated terms

EDITOR'S NOTE: To be defined during project drafting

CAB Conformity Assessment Body

5 General concepts

5.1 Evaluation actors

EDITOR'S NOTE: Even though it has been decided that this standard won't define a conformity assessment scheme, it is considered important to introduce the relevant actors, and the relationships among them. We will add recommendations for each of those actors, according to the best practices in conformity assessment

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 that, based on the specifications, requirements and methods defined in standards like this one, provide the rules for certifying relevant products and/or services.

— Certification Assessment Body (CAB)

— Testing Laboratory (TL)

— Evaluation methodology

— Product Manufacturer

— Customer

Each of those actors are describe in following subclauses.

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

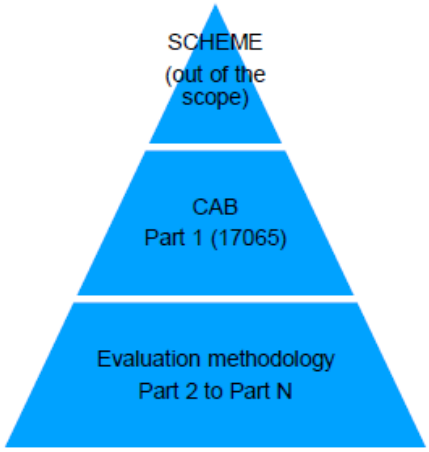

Figure 1 — Relationship among Scheme, CAB and Evaluation Methodology

5.1.2 Conformity assessment bodies

5.1.2.1 Certification body

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.

5.1.3 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, 5.4 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.

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

Evaluators can perform two different types of conformity evaluation processes:

— The conformity with the certification scheme based on this standard (out of the scope – certification body)

— The testing of functional and security requirements described in the appropriate application profile (testing laboratory)

5.1.4 Evaluation methodology

TBD

5.1.5 Product manufacturer

TBD

5.1.6 Customer

TBD

5.2 Evaluation process

EDITOR'S NOTE: explaining the relationships and workflow since the product manufacturer (customer) decides to start the evaluation of the TOE by a TL in order to comply with some additional requirements provided by, for example, a CAB)

Before performing the evaluation's tests, the Customer or the TOE manufacturer will have to provide a document titled "Security Declaration of the TOE" (see clause 5.3), that will help the TL to detect the points where the security evaluation shall focus. It may happen that the Customer and/or the TOE

manufacturer may need the assistance of a third-party consultant, or even the TL selected, to define such a document.

The evaluation process is set on three different phases:

— Phase 1: functional evaluation (see clause 5.4.2)

— Phase 2: functional boundaries testing (see clause 5.4.3)

— Phase 3: attack detection testing (see clause 5.4.4)

Depending of the biometric modality 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 modality, 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 insurance (basic, substantial and high) defined in the EU CSA.

5.3 Security declaration of the TOE (SD_TOE)

At beginning of the assessment, the evaluator needs to read the Security Declaration of the TOE (SD_TOE) provided by the Customer and/or TOE manufacturer. 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 SD_TOE 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 SD_TOE 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
    2) Description of the use of the product to be evaluated
    3) Description of the intended use environment
    4) Description of dependencies
    5) Description of typical users
    6) Description of the TOE
c) Description of the technical operating environment
    1) Asset to protect by the TOE
d) Description of threats
e) Description of the security functions of the TOE
f) Threats coverage

In addition to this content, the SD_TOE shall also include those additional items required by the applicable application profile (see clause 6.6).

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

5.4 Evaluation phases

5.4.1 General

Each biometric modality part of this standard serie (part 4 to N) shall describe the different test 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.

Eventually, note that the settings values and the decision criteria for each test are described in the corresponding application profile in annex.

5.4.2 Phase 1: Functional evaluation

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.

5.4.3 Phase 2: Functional boundaries testing

The main target of this phase is to learn about the TOE, as to be able 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 3 tests.

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

5.4.4 Phase 3: Attack-detection evaluation

The main target of phase 3 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 3 for the TOE. This will be determined by analysing that the attack is not exceeding the maximum attack potential for the TOE evaluation.

6 Definition of application profiles

EDITOR'S NOTE: We may find a better name for the "application profile" in the line of naming it as if "Security Targets (from CC)" are being defined.

6.1 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 modality part of this standard serie.

Application profiles are the baseline for getting a conformity with this standard serie. Indeed, a specific product can demand an evaluation process to a testing laboratory to get a conformity with the according standard of this serie (depending of the biometric modality used by the TOE) AND a specific application profile AT a certain level of insurance (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 serie. Otherwise, a testing laboratory can't attest a conformity with this standard serie.**

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 insurance: 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 serie and the specific application profile.

6.2 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

— The biometric modality used

— A general usage description of the TOE

— A general architecture of the TOE

— The capture devices and the environment of usage of the TOE

6.3 Evaluation levels of assurance

This part intends to give the main guidelines concerning the possible evaluation levels of insurance for the targeted product range. For being compliant with the EU CSA, this standard serie will consider three levels: basic, substantial and high.

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 XXXXX (text of the EU Commission with that relationship).

The application profile shall follow the following structure to present the guidelines for the evaluation levels of insurance:

Table 1 — Structure for presenting the guidelines for the evaluation levels of insurance in an application profile

Levels	Minimum requirements for attack detection testing	Knowledge of the TOE	Time elapsed to perform the evaluation (writing the SD_TOE, creating attacks, testing and writing the report)	Passing criteria (for all phases)
Basic (Level 1)	*Number of attacks taken into account*	*Creation or not of a SD_TOE document*	*Number of working days*	*Maximum classification error rates percentage for performances* *Maximum classification error rates percentage for attack detection OR minimum resilience against attack level (depend of the application profile)*
Substantial (Level 2)	*Number of attacks taken into account*	*Creation or not of a SD_TOE document*	*Number of working days*	*Maximum classification error rates percentage for performances* *Maximum classification error rates percentage for attack detection OR minimum resilience*

				against attack level (depend of the application profile)
High (Level 3)	*Number of attacks taken into account*	*Creation or not of a SD_TOE document*	*Number of working days.*	*Maximum classification error rates percentage for performances* *Maximum classification error rates percentage for attack detection OR minimum resilience against attack level (depend of the application profile)*

6.4 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 precised 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.

6.5 Functional requirements

6.5.1 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 1 and phase 2 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-match 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 2 — Decision criteria for functional requirements testing

VARIABLE	OP.	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 insurance. Thus, if the application profile intends to reach the three different level of insurance, the decision criteria for each functional tests shall be defined for each level of insurance (in different subclauses in the application profile).

6.5.2 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.

6.6 Security requirements

6.6.1 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 3 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 SD_TOE, 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 3 — Decision criteria for security requirements testing

VARIABLE	OP.	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 insurance. Thus, if the application profile intends to reach the three different level of insurance, the decision criteria for each security tests shall be defined for each level of insurance (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).

6.6.2 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.

6.6.3 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.

6.7 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 3).

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 insurance if the application profile intends to apply for different evaluation levels of insurance.

Bibliography

[1] EN XXXX, *Title of reference*