SLOVENSKI STANDARD
SIST-TS CEN/TS 18212-5:2026

01-oktober-2026

Osebna identifikacija - Zahteve za biometrične izdelke - 5. del: Biometrija obraza

Personal identification - Requirements for biometric products - Part 5: Face biometrics

Persönliche Identifikation - Anforderungen an biometrische Produkte - Teil 5: Biometrische Gesichtserkennung

Identification personnelle - Exigences relatives aux produits biométriques - Partie 3 : Biométrie faciale

Ta slovenski standard je istoveten z: **CEN/TS 18212-5:2026**

ICS:

35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

SIST-TS CEN/TS 18212-5:2026 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 18212-5

June 2026

ICS 35.240.15

English Version

Personal identification - Requirements for biometric products - Part 5: Face biometrics

Identification personnelle - Exigences relatives aux produits biométriques - Partie 3 : Biométrie faciale

Persönliche Identifikation - Anforderungen an biometrische Produkte - Teil 5: Biometrische Gesichtserkennung

This Technical Specification (CEN/TS) was approved by CEN on 24 May 2026 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 18212-5:2026 E

Contents

Page

European foreword

This document (CEN/TS 18212-5:2026) has been prepared by Technical Committee CEN/TC 224 "Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment", the secretariat of which is held by AFNOR.

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

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

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. Many online services can now be found, 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, inclusive and auditable way. Even though some of those services, in some countries, were deployed using public key infrastructures (PKIs), as recommended by eIDAS [1], for a significant part of the population.

Biometric recognition has been considered as a technology to solve the binding between the system and the consumer. Adding biometric recognition to all kinds of systems is a common practice nowadays.

Readers, especially those not too much familiar with the biometrics verification process, may find it interesting to read Clause 2 of BSI TR 03166 [2], which can be found in https://www.bsi.bund.de/dok/TR-03166-en.

In this context, service providers and administrations define their own requirements, select the products and deploy the solution. On the other hand, manufacturers 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 benefits 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 applicable standards.

NOTE ISO/IEC17000 and related standards are examples of applicable conformity assessment standards.

This document 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 document has been with consideration for GDPR [3] principles.

Application profiles (*APs*) are targeting the evaluation of a specific range of products using biometric recognition. *APs* are the baseline for checking conformity with the CEN/TS 18212 series [4]. Indeed, a product manufacturer (PM), product vendor (PV) or sponsor can ask a conformity assessment body (CAB) for the evaluation of a specific product to check its conformity according to the CEN/TS 18212 series [4] and a specific *AP* at a certain *level of assurance* (basic, substantial or high).

The specifications given in this document are based on EN ISO/IEC 15408-1 [5], CEN/TS 18099 [6], ISO/IEC 19989-3 [7], ISO/IEC 19795-1 [8] and the ISO/IEC 170xx family of standards. These standards specify processes dealing with evaluation and certification of products and services, either related to their performance or to their security.

These objectives are reached by the development of a multipart Technical Specification (i.e. the CEN/TS 18212 series [4]) with the following structure:

— Parts 1-3: Defining the generic principles and methodologies, not requiring a biometric mode specific approach. In particular, these parts are:
  — Part 1: General requirements and application profile definition;
  — Part 2: Interoperability tests;
  — Part 3: Functionality evaluation methodology.

— Parts 4-n: Planned future parts of the CEN/TS 18212 series, defining the particularities of each biometric mode (e.g. specific *TESTs*, specific requirements) and containing a set of *APs*, that establish the *TESTs* and requirements applicable for a specific application and context. Those *APs* are addressed in individual annexes, following the structure provided in CEN/TS 18212-1 [9]. For example, these parts can be:

  — Part 4: Fingerprint biometrics

  — Part 5: Face biometrics (i.e. this document)

This document is focused on the definition of the catalogue of *TESTs* to be executed in products with face biometric recognition, as well as a set of *APs* for products using this technology.

1 Scope

The CEN/TS 18212 series [4] specifies a generic framework for the establishment of requirements and their evaluation methodology for biometric products. The requirements depend on the biometric mode considered, and are adapted to each scenario, through the definition of a variety of application profiles.

The CEN/TS 18212 series [4] specifies the evaluation methodology, the individual *TESTs*, and the application profiles (with their particular requirements).

This document is focussed on face biometrics, and provides the specifics of this biometric mode for the application of all the specifications provided in parts 1 till 3 from CEN/TS 18212 series [4]. It also defines a set of application profiles, that detail the applicable *TESTs*, the evaluation parameters and the assessment criteria.

In detail, this document defines, for face biometric products:

— general aspects of a face *biometric product*;

— common resources needed for the evaluation;

— each of the possible *TESTs* to be applied;

— application profiles for different kinds of face biometrics products.

NOTE 1 National regulations and requirements can apply.

NOTE 2 Regarding biometrics for public sector applications, see also BSI TR 03121 [10] which can apply.

NOTE 3 For an overview of sectors addressed in the Cybersecurity Act, see Regulation (EU) 2019/881[11].

NOTE 4 This part defines all potential *TESTs* that could be applicable when evaluating the functionality of a *biometric product* using this biometric mode. It will be the relevant *application profile* (3.1.1), the one that will specify which of these *TESTs* are applicable.

The following topics are left out of the scope of this document:

— Vulnerability assessment of the storage system used for the biometric reference/s.

— Vulnerability assessment of communication protocols and interfaces dealing with the operation of the *biometric product*.

— Evaluation of the performance of human operators in terms of identity proofing.

— Validation of documents providing the biometric reference.

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 19794-5, *Information technology — Biometric data interchange formats — Part 5: Face image data*

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

ISO/IEC 19795-2, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

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 29794-5, *Information technology — Biometric sample quality — Part 5: Face image data*

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

ISO/IEC 39794-5, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*

EN ISO/IEC 2382-37, *Information technology - Vocabulary - Part 37: Biometrics (ISO/IEC 2382-37:2022)*

EN ISO/IEC 15408-1, *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model (ISO/IEC 15408-1:2009)*

EN 17640, *Fixed-time cybersecurity evaluation methodology for ICT products*

EN ISO/IEC 18045, *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation (ISO/IEC 18045:2022)*

CEN/TS 18099, *Biometric data injection attack detection*

CEN/TS 18212-2, *Personal identification - Requirements for biometric products - Part 2: Interoperability tests*

CEN/TS 18212-1, *Personal identification - Requirements for biometric products - Part 1: General requirements and application profile definition*

CEN/TS 18212-3, *Personal identification - Requirements for biometric products - Part 3: Functionality evaluation methodology*

ISO/IEC 19795 (all parts), *Information technology — Biometric performance testing and reporting*

ISO/IEC 19989, *Information security — Criteria and methodology for security evaluation of biometric systems*

ISO/IEC 30107 (all parts), *Information technology — Biometric presentation attack detection*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CEN/TS 18212-1, CEN/TS 18212-3, ISO/IEC 19795 (all parts), ISO/IEC 30107 (all parts), ISO/IEC 19989, EN ISO/IEC 2382-37 and the following apply.

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1 Terms

3.1.1
application profile
AP
APs
definition of a target of evaluation (TOE) and set of specifications and requirements for the evaluation of such TOE according to a certain application

Note 1 to entry: The definition and basic content of an *AP* (3.1.1) is given in CEN/TS 18212-1:2026 [12].

3.1.2
attack potential
measure of the effort needed to exploit a vulnerability in a target of evaluation (TOE)

Note 1 to entry: The effort is expressed as a function of properties related to the *ATTACKER* (3.2.1) (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

[SOURCE: EN ISO/IEC 15408-1 [5]]

3.1.3
biometric product
biometric system
product that contains one or more biometric subsystems for achieving its designed functionality

Note 1 to entry: This document is focussed on the evaluation of biometric products, so if a *biometric product* (3.1.3) contains more than one biometric systems, the evaluation will have to be applied to each of those subsystems, being each of them a target of evaluation (TOE).

3.1.4
biometric subsystem
set of modules that perform the biometric functions within the *biometric product* (3.1.3)

EXAMPLE Examples of biometric functions are quality checking, pre-processing, comparison, *presentation attack detection* (3.1.10) methods.

[SOURCE: CEN/TS 18212-3 [13]]

3.1.5
evaluation technical report
ETR
document (or set of documents) that present the way the evaluation has been carried out and the results achieved

Note 1 to entry: The definition and basic contents of the ETR can be found in CEN/TS 18212-1 [9].

3.1.6
evidence
information needed by a third party (e.g. and auditor) to verify that the *TEST* (3.2.41) has been executed correctly, including the equipment and materials used

EXAMPLE In the case of a Phase 3 attack using masks, the *evidence* (3.1.6) is expected to show the mask by itself and the mask applied to the *ATTACKER* (3.2.1), as well as the a-priori similarity score achieved by *REF_APP* (3.2.32).

3.1.7
level of assurance
LoA
LoAs
degree of confidence or certainty in the accuracy and reliability of a claimed identity, particularly in digital systems and online transactions

Note 1 to entry: In the context of the European Union, the definition of the LoAs is given by the CSA regulation[11].

Note 2 to entry: A *biometric product* (3.1.3) that reaches a certain LoA, means that it is robust against all attacks with attack potentials below such LoA.

3.1.8
liveness detection
mechanism of the TOE that is in charge of detecting if the *SUBJECT* (3.2.37) is alive, being a subset of the TOE's *presentation attack detection* (3.1.10) mechanisms

Note 1 to entry: The liveness detection mechanism can require the *SUBJECT* (3.2.37) to perform some kind of response to some challenges, as to be able to force the presentation of a *proof-of-life* (3.1.12) by the *SUBJECT* (3.2.37).

3.1.9
lookalike
lookalikes
look-alike
someone or something that is similar in appearance to someone or something

Note 1 to entry: In the context of this document, *SUBJECT* (3.2.37) that is very similar in appearance to another *SUBJECT* (3.2.37), showing a similarity score higher or equal to *BONAFIDE_ALIKE_TH* (3.2.8) using *REF_APP* (3.2.32).

Note 2 to entry: This definition includes, for example, twins, very similar siblings, etc.

3.1.10
presentation attack detection
PAD
automated discrimination between bona-fide presentations and biometric presentation attacks

Note 1 to entry: *PAD* (3.1.10) cannot infer the biometric capture *SUBJECT* (3.2.37)'s intent.

[SOURCE: ISO/IEC 30107-1 [14]]

3.1.11
presentation attack instrument
PAI
PAIs

biometric characteristic or object used in a biometric presentation attack

Note 1 to entry: The set of PAI includes artefacts but would also include lifeless biometric characteristics, (stemming from dead bodies) or altered biometric characteristics (e.g. altered fingerprints that are used in an attack).

[SOURCE: ISO/IEC 30107-1 [14]]

3.1.12
proof-of-life
evidence (3.1.6) provided to the biometric capture system that allow to determine that the biometric sample captured is coming from a living *SUBJECT* (3.2.37)

Note 1 to entry: A *proof-of-life* (3.1.12) can be required by a *biometric product* (3.1.3), as to avoid presentation attacks, either by direct presentation, or by digital injection.

3.1.13
testing laboratory
TL
TLs
entity that will carry out the evaluation of a TOE using the methodology and *TESTs* (3.2.41) defined in this Technical Specification series

3.2 Symbols and parameters

3.2.1
ATTACKER
ATTACKERs
SUBJECT (3.2.37) that interacts with the TOE with the intention to attack it, either to impersonate a *BONAFIDE_SUBJECT* (3.2.7), or to obfuscate its identity

Note 1 to entry: The *ATTACKER* (3.2.1) only plays a relevant role in Phase 3.

Note 2 to entry: In Phase 3 *TESTs* (3.2.41), the evaluator acts as an ATTACKER.

3.2.2
ATTACKER_BONAFIDE_SIM_TH
threshold for the similarity between an *ATTACKER* (3.2.1) and a *BONAFIDE_SUBJECT* (3.2.7), used to determine if the *ATTACKER* (3.2.1) has reached enough similarity with the *BONAFIDE_SUBJECT* (3.2.7) that is intended to be attacked

Note 1 to entry: This threshold only plays a role in Phase 3.

3.2.3
ATTACKER_BONAFIDE_ALIKE_TH
threshold for the similarity between an *ATTACKER* (3.2.1) and a *BONAFIDE_SUBJECT* (3.2.7), as to consider them as *lookalikes* (3.1.9)

3.2.4
ATTEMPT
ATTEMPTs
each of the individual interactions between the *SUBJECT* (3.2.37) and the TOE within a *TRIAL* (3.2.46)

3.2.5
BONAFIDE_LOW_SIM_TH
threshold to determine if two test subjects are very different from each other

Note 1 to entry: This threshold only plays a role in T2-1-2.

3.2.6
BONAFIDE_SIM_TH
threshold to determine that two test subjects present an acceptable level of similarity, according to *REF_APP* (3.2.32)

Note 1 to entry: This threshold only plays a role in Phase 2.

3.2.7
BONAFIDE_SUBJECT
BONAFIDE_SUBJECTs
SUBJECT (3.2.37) that interacts with the TOE with a legitimate use and without any intention to attack it

Note 1 to entry: For Phase 2, *SUBJECT* (3.2.37) and *BONAFIDE_SUBJECT* (3.2.7) are equivalent. In Phase 3, the *BONAFIDE_SUBJECT* (3.2.7) is the one to be impersonated by the *ATTACKER* (3.2.1).

3.2.8
BONAFIDE_ALIKE_TH
threshold to determine if two *BONAFIDE_SUBJECTs* (3.2.7) are considered to be *lookalikes* (3.1.9)

Note 1 to entry: This threshold only plays a role in Phase 2.

3.2.9
ERROR
result from the TOE indicating that the biometric comparison has not been carried out

Note 1 to entry: The ERROR could not be indicated directly by the TOE, but by the *TL* (3.1.13) when considering that a pre-defined *TIMEOUT* (3.2.45) has happened without getting any response from the TOE.