SLOVENSKI STANDARD
SIST-TS CEN/TS 17661:2022

01-februar-2022

Osebna identifikacija - Evropsko vodilo za vpis biometričnih osebnih dokumentov (EEG)

Personal identification – European enrolment guide for biometric ID documents (EEG)

Persönliche Identifikation - Europäischer Enrolmentguide für biometrische ID-Dokumente (EEG)

Ta slovenski standard je istoveten z: **CEN/TS 17661:2021**

ICS:

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

SIST-TS CEN/TS 17661:2022 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 17661

November 2021

ICS 35.240.15

English Version

Personal identification - European enrolment guide for biometric ID documents (EEG)

Identification des personnes - Guide d'enrôlement européen pour les documents d'identité biométriques (EEG)

Persönliche Identifikation - Europäischer Enrolmentguide für biometrische ID-Dokumente (EEG)

This Technical Specification (CEN/TS) was approved by CEN on 16 August 2021 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, Turkey 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 17661:2021 E

Contents

Page

European foreword

This document (CEN/TS 17661:2021) 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, Turkey and the United Kingdom.

Introduction

Over the past decade, many EU Member States introduced MRTD supported traveller processes. During this time, lessons have been learned and experience has been gained on several application aspects of newly introduced technologies. One key component of any MRTD inspection system is the biometric comparison of the document holder with the reference data. In addition to passports and ID cards, biometric data are used for documents other than eMRTD as well, including Residence Permits, Visas and Drivers Licenses. This document aims to compile these lessons learnt and present best practice in capturing facial and fingerprint images, and to improve the biometric samples at the point of capture from the enrolee.

During the last few years, biometric comparison algorithms reached new performance levels and even more improvements can be expected. However, every system can only be as good as the data it is based on. Therefore, the quality of reference data has superior importance. The better the enrolment of biometric data, the lower the error rates to be expected in any MRTD based application. Lower error rates lead to a higher degree of automation, increase throughput and security, improve the traveller experiences, and, finally, save resources. So, it is worth investing in enrolment of high quality facial images as well as of fingerprint images.

The enhanced use of new technologies for identity and document inspection means that precise criteria is set out for the enrolment and inspection processes. The enrolment process for biometric identifiers is crucial in order to guarantee a successful verification at document inspection. This document presents guidelines for the enrolment of an enrolee's biometric face and fingerprint characteristics, which can be used for identity documents.

With the amendment of Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders (OJ L 74 of 18 March 2017 p.1-7) the following provisions have been inserted:

— for passports and travel documents containing a storage medium as referred to in Article 1(2) of Council Regulation (EC) No 2252/2004, the authenticity of the chip data shall be checked;

— where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with Regulation (EC) No 2252/2004 shall be verified. Where possible, such verification is carried out in relation to travel documents not covered by that Regulation.

This concludes that in case of doubt a verification of the facial or the fingerprint image shall be carried out. In order to achieve a successful verification, the following guidelines have been developed for enrolment of these biometric data. The guidelines are intended to assist the responsible parties to achieve the best quality of biometric enrolment in order to:

— create identity documents with high quality facial images integrated within the document and stored on the chip in combination with high quality fingerprint images;

— prevent identity fraud by ensuring the integrity of the enrolment process;

— reduce false and increase true matching of facial and fingerprint images.

1 Scope

This document consolidates information relating to successful and high quality biometric enrolment processes of facial and fingerprint systems, while indicating risk factors and providing appropriate mitigations. This information supports decisions regarding procurement, design, deployment and operation of these biometric systems.

This document provides guidance on:

— capturing of facial images to be used as reference images in identity and secure documents;

— capturing of fingerprint images to be used as reference images in identity and secure documents;

— data quality maintenance for biometric reference data;

— data authenticity maintenance for biometric reference data.

The document addresses the following aspects which are specific for biometric reference data capturing:

— biometric data quality and interoperability ensurance;

— data authenticity ensurance;

— morphing and other presentation attack detection as well as other unauthorized changes;

— accessibility and usability;

— privacy and data protection;

— optimal enrolment design.

The following aspects are out of scope:

— IT security;

— data capturing for verification purposes, e.g. in ABC gates;

— capturing biometric data for enrolment in other systems different from data enrolment for integration in secure MRTD, like entry/exit systems.

This document consolidates the role of the enrolment process in a biometric system and differentiates the enrolment from the authentication, while mentioning key factors of the enrolment process that are feature independent.

Interests of the existing stakeholders are broken down and provide an insight on different views of the enrolment. In addition, organisational enrolment approaches are covered.

This document is not concerned with IT requirements or the capturing of biometric data for inspection, identification or verification purposes without the required step of creating an identity document using the captured data.

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 17054:2019, *Biometrics multilingual vocabulary based upon the English version of ISO/IEC 2382-37:2012*

IEC 61966-2-1, *Multimedia systems and equipment — Colour measurement and management — Part 2–1: Colour management — Default RGB colour space — sRGB*

ISO/IEC 10918-1, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*

ISO/IEC 14496-2:2004, *Information technology — Coding of audio-visual objects — Part 2: Visual*

ISO/IEC 15444-1, *Information technology — JPEG 2000 image coding system — Part 1: Core coding system*

ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data*

ISO/IEC 2382-37:2017, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 39794-4, *Information technology — Extensible biometric data interchange formats — Part 4: Finger image data*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 17054:2019, ISO/IEC 2382-37:2017 and the following apply.

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

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

3.1
attended capture
acquisition of a biometric characteristic of an enrolee, while providing guidance

Note 1 to entry: Guidance is usually provided by an enrolment officer during live enrolment.

3.2
attendant
person, remote or automated system assisting the enrolment officer in obtaining the best available quality biometric sample during capture through the procedures defined for enrolees with accessibility needs or special requirements related to their age, gender, and religious observance

EXAMPLE 1 The automatically adjustable chair, detecting eye positions, while being removable for wheelchair access.

EXAMPLE 2 Vocal assistance to guide partially sighted enrolees.

3.3
auditor
individual verifying the execution of the enrolment process, capture and registration, by checking against the enrolment protocol

3.4
automated controlled capture
acquisition of an enrolee's biometric characteristics, controlled by an automated system, not by personnel

Note 1 to entry: The most common automated application for facial images is a photo booth.

3.5
biometric enrolee
individual providing a biometric sample to the capture system

3.6
capture
obtain contemporary signal(s) of biometric characteristic(s) from biometric enrolee(s)

3.7
designer and developer
entity designing the capture and/or registration system, service, process and the interaction protocol for the enrolee

Note 1 to entry: Designer and developer create the service for production and distribution of any token used as storage for biometric references or a pointer to where biometric references are stored.

3.8
duty officer
individual providing technical and operational advice and guidance to an enrolment officer

3.9
enrolment
action of storage of a biometric capture data record in accordance with the biometric enrolment policy

Note 1 to entry: The process of enrolment is to be distinguished into two subprocesses, capture and registration.

3.10
enrolment authority
national entity being responsible for the capture and registration of biometric features of an enrolee and being liable for the processed data until the creation of the corresponding identity document

Note 1 to entry: The enrolment authority performs any required quality checks, including data authenticity checks and enrolee identity validation.

Note 2 to entry: The enrolment authority is responsible for delivering the identity document, regardless how this process is defined.

EXAMPLE Fraudulent attempts to prevent may be an enrolees claiming to have lost their identity document and asking for an issuance of a new one, or the enrolee, being in the process of document renewal or creation, submitting non-matching biometric data.

3.11
enrolment officer
individual interacting with enrolees to provide information regarding the enrolment process and supporting operators in case of difficulties as the executing part of the enrolment authority

Note 1 to entry: The enrolment officer is responsible for the entire capture and registration process, even if different personnel and multiple sessions take place.

Note 2 to entry: The enrolment officer's tasks may differ between capture and registration. The following examples illustrate possible tasks during each enrolment subprocess.

EXAMPLE 1 During capture, the enrolment officer oversees one or multiple enrolment stations, being responsible for the secure and effective enrolment service. The enrolment officer ensures the day-to-day maintenance of equipment used during the enrolment and ensures the quality of the enrolment feature captured by the sensor or camera, meeting the enrolment standards, usually through requesting the enrolee to re-enrol if the standard is not achieved, noting any exceptional circumstances. This assistance can be done by a physical person but also by an automatic enrolment system adaption or video remote assistance.

EXAMPLE 2 During registration, the enrolment officer stores the captured biometric feature to the corresponding identity of the enrolee. If the capture happened during a different session, a verification of the enrolee's biometric feature is mandatory, reducing mistakes or possible angles for an attack.

3.12
facial image
visual representation that includes the frontal part of the head of an enrolee, including hair if any, the neck, and possibly the top of the shoulders

Note 1 to entry: A facial image may be stored in a digital file or be printed. In cases where the difference matters, the terms "digital facial image" and "printed facial image" are used, respectively.

Note 2 to entry: The term "facial image" describes the same concept as the term "face image" used throughout ISO documents.

Note 3 to entry: The terms "facial image" and "portrait" are used equivalently throughout this document.

3.13
facial region
region from crown to chin and from the left ear to the right ear, disregarding the background of the image

3.14
fixed enrolment
enrolment through stationary capture and registration stations set up at one location

3.15
identity document
document issued by a state authority that can be used to prove a person's identity

EXAMPLE National ID card, passport, visa, resident permits.

3.16
imaging system
technical system that reproduces an image

3.17
in-house enrolment
capture and registration performed by the enrolment authority, using the processed data in a business-oriented application

3.18
Key Performance Indicator
KPI
metric quantifying one or more aspects of the successful operation of a process

3.19
live capture
capture without use of an intermediate medium

3.20
mandatory enrolment
enrolment that is prerequisite for the use of the product or service by any user

EXAMPLE A passport may be a requirement for travelling to different countries. A facial image is a requirement for a valid passport.

3.21
mobile enrolment
enrolment through moveable capture and registration stations, that can be set up at multiple locations

3.22
morphing attack
abuse of an authentic document, in which the biometric features of the document holder are merged with biometric features of at least one other person, resulting in a manipulated facial or fingerprint image used in the ID document that contains biometric features of two or more persons

3.23
multiple location enrolment
capture and registration procedures take place at different locations

Note 1 to entry: Multiple location enrolment may need more sophisticated security measures, due to the split over multiple sessions, to provide a flawless chain of proof.

3.24
non-professional capture
acquisition of an enrolee's biometric characteristics in an uncontrolled environment

EXAMPLE The environment is uncontrolled if either camera, lighting, computer or enrolment software is non-professional or, in case of facial image capturing, a non-professional photographer.

3.25
operator
individual organizing the capture and registration service, being responsible to the enrolment authority

Note 1 to entry: Quality and security of the enrolment service are the key areas of responsibility of the operator.

EXAMPLE If the KPIs, including quality and performance metrics, fall outside the agreed targets, the operator takes remedial measures.

3.26
optional enrolment
enrolment is no requirement for the use of the product or service by the user

3.27
outsourced enrolment
capture and registration performed by a service provider carrying out the enrolment

3.28
performance manager
individual monitoring the procedure of the capture and registration process, proposing and reporting back on corrective actions, if the specified criteria are not met

3.29
personal assistant
individual or automated system providing support for the enrolee

EXAMPLE 1 For human assistance: Translation of instructions from the enrolment officer, support for a handicapped enrolee, fulfilling a legal requirement, such as being present during the enrolment of a child.

EXAMPLE 2 For an automatic capture system adaption: Translation of instructions, age detection.

3.30
photo booth
automated or semi-automated system for digitally capturing facial images, and securely transferring them to the authority, that encloses the enrolee in a highly-controlled lighting environment, consists of a camera, lighting, and peripheral devices, and has an entrance protected against ambient light

Note 1 to entry: In some use cases, a semi-automated photo booth can be located in a supervised area with the operator providing assistance during the capture process. Therefore, the photo booth can be equipped with partial masking or semi-transparent materials which can be removable.

3.31
photo kiosk
automated or semi-automated system for digitally capturing facial images in a bureau-environment that consists of a camera and lighting and usually has a separate panel placed behind the enrolee to provide the required background but is otherwise open

3.32
photo studio
licensed, professional working environment run by photographers, functioning as operators, taking facial images using professional equipment

Note 1 to entry: Professional equipment usually refers to the camera and lighting setup, being the most relevant for a compliant portrait.

3.33
printed image capture
physical acquisition of an enrolee's biometric characteristic, to be scanned and registered by the enrolment authority

3.34
professional capture
acquisition of an enrolee's biometric characteristics in a controlled environment

Note 1 to entry: Professional capture of facial images is usually done by a photographer or a properly set up photo booth.

3.35
registration
operation of (1) processing an application for identity document, and storing and binding a previously captured biometric feature to a claimed identity, requiring presence of both the enrolee and the enrolment officer, and (2) verifying the claimed identity matches the enrolee, requiring presence of the enrolment officer

Note 1 to entry: The two steps, i.e. (1) processing of the application and storage and binding a previously captured biometric feature to a claimed identity and (2) verification may take place at different places and different moments depending on enrolment procedures (e.g. verification step may be performed later by dedicated and duly trained and accredited staff).

3.36
regulator
individual assuring the capture and registration process is operated according to legislation acts, relative contract documents and instructions

3.37
relying party
entity using the biometric data obtained from the enrolment service in a biometric recognition service as part of a business-oriented application

3.38
remote enrolment
enrolment through online capture and registration methods, enabling secure data transfer

3.39
secure capture
human or automatic supervised live capture with PAD and no unsecured intermediate storage

3.40
semi-attended capture
acquisition of a biometric characteristic of an enrolee, by one enrolment officer or third party operator overseeing one or multiple enrolment processes

EXAMPLE 1 A possible third party operator could be a studio photographer.

EXAMPLE 2 One or many enrolment officers using the same capturing environment not directly located at their workspace.

3.41
Service Level Agreement
SLA
agreement between a service provider and a customer defining a target level of service, mutual responsibilities of service provider and customer, together with other requirements for the delivery of a service

3.42
single location enrolment
capture and registration procedures take place at the same location, irrelevant of the chosen session model

3.43
specialist support staff
trained attendant(s) present at the enrolment session on behalf of the enrolment authority or operator to assist with the enrolment of enrolees with disabilities, or to fulfil service or legal requirements in respect of gender, religious observance, or age of the enrolee

3.44
supervised enrolment
enrolment which is observed and/or directed by a human, which may or may not be supported by an automatic system

3.45
unaware enrolment
enrolment occurring without the enrolee recognizing

EXAMPLE Relevant for surveillance or tracking.

3.46
uncontrolled capture
acquisition of an enrolee's biometric characteristics without any kind of supervision

3.47
vendor
entity providing hardware, software and technical support for the capture and registration process

Note 1 to entry: The support is either provided directly or through an agent.

EXAMPLE Providing upgrades or rectification of faults.

4 Abbreviated terms

CCTV	Closed Circuit Television
CSD	Camera to Subject Distance
EVZ	Eye Visibility Zone
FAP	Fingerprint Acquisition Profile
FMR	False Matching Rate
FNMR	False Non-Matching Rate
FTAR	Failure to Acquire Rate
FTER	Failure to Enrol Rate
FTIR	Frustrated Total Internal Reflection
GDPR	General Data Protection Regulation
IED	Inter Eye Distance
KPI	Key Performance Indicator

MRTD	Machine-Readable Travel Document
NFIQ	NIST Fingerprint Image Quality
PAD	Presentation Attack Detection
SLA	Service Level Agreement
SNR	Signal to Noise Ratio
TFT	Thin Film Transistor
WSQ	Wavelet Scalar Quantization

5 Enrolment and use of reference data in a biometric system

Biometric enrolment systems have many elements in common. Captured biometric samples are acquired from an enrolee by a sensor. The sensor output is sent to a processor that extracts the biometric features, the distinctive but repeatable measures of the sample, discarding all other components. The resulting image or images are registered by the responsible authority and may be used to:

— confirm the identity of an enrolee claiming for renewal; or

— confirm the identity of an enrolee claiming having lost or been stolen its identity document; or

— issue an Identity Document in which they are stored; or

— detect an identity substitution in the course of identity document renewal (e.g. submission of a morphed biometric data); or

— confirm the identity of the person to deliver the identity document.

Using the collected biometric sample for biometric recognition encompasses both:

— biometric identification;

— biometric verification.

Biometric verification can be used to conduct a 1:1 comparison of a captured biometric template (i.e. the biometric claim) against one stored on a card, mobile device, or database. Biometric identification can be used to deduplicate identity records during registration (i.e. to perform a duplicate biometric enrolment check).

Verification of an identity claim, or confirmation of identity is achieved using a subsequent probe biometric sample which is compared to the reference one. A decision regarding the biometric claim is made based upon the similarities or dissimilarities between the features of the biometric probe and those of the reference compared. For more detailed information about the architecture of biometric systems see ISO/IEC TR 29196.