SLOVENSKI STANDARD
kSIST-TS FprCEN/TS 18139:2025

01-januar-2025

Osebna identifikacija - Evropski vodnik za aplikacije biometričnega prepoznavanja na podlagi osebnih dokumentov (ERG)

Personal identification - European guide for biometric recognition applications based on ID documents (ERG)

Persönliche Identifikation - Europäischer Leitfaden für Verifikationsanwendungen auf der Grundlage von ID-Dokumenten (EVG)

Identification des personnes - Guide européen pour les applications de reconnaissance biométrique basées sur des documents d'identité (ERG)

Ta slovenski standard je istoveten z: **FprCEN/TS 18139**

ICS:

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

kSIST-TS FprCEN/TS 18139:2025 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT
FprCEN/TS 18139

November 2024

ICS 35.240.15

English Version

Personal identification - European guide for biometric recognition applications based on ID documents (ERG)

Identification des personnes - Guide européen pour les applications de reconnaissance biométrique basées sur des documents d'identité (ERG)

Persönliche Identifikation - Europäischer Leitfaden für Verifikationsanwendungen auf der Grundlage von ID-Dokumenten (EVG)

This draft Technical Specification is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/TC 224.

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

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. FprCEN/TS 18139:2024 E

Contents

Page

European foreword

This document (FprCEN/TS 18139:2024) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document is currently submitted to the Vote on TS.

Introduction

Biometric reference data for ID documents meanwhile are highly standardized by ISO, ICAO, and CEN. Within CEN, this work is done by TC 224/WG 18 in close cooperation with the Article 6 Technical Subgroup and FRONTEX. Several International Standards, in particular ISO/IEC 19794 series and ISO/IEC 39794 series, achieve technical interoperability of biometric data.

With CEN/TS 17661 [1] the enrolment of biometric data for identity documents has been profiled specifically for European needs. However, biometric data is captured in many other situations as well, even in the context of ID documents, in particular for verification applications like automated or manual border control, or temporary enrolment into entry/exit systems. This gap shall be addressed by this TS.

During the development of the TS, a close cooperation between WG18 and the EU has been maintained to ensure that the needs of the Member States are exactly met.

The document gives recommendations for

- Capturing of facial images for verification applications mainly using reference data stored in identity documents or traveller/visa databases, covering data quality and interoperability, data authenticity, morphing and presentation attack detection in several environments,

- Capturing of fingerprint images for verification applications mainly using reference data stored in identity documents or traveller/visa databases, covering data quality and interoperability, data authenticity, and presentation attack detection in several environments, and

- Processes handling such biometric data for verification and identification purposes considering security as well as privacy aspects.

This document covers biometric recognition applications based on ID documents. Biometric recognition applications within the frame of this document are corresponding to the definition of biometric recognition systems in ISO/IEC 2382-37:2022 encompassing identification and verification systems. This means that biometric recognition applications should be considered as a subsystem of a complete identity verification system. Identity verification systems can be ABC gates, inspection systems, mobile phones etc.

1 Scope

This document defines requirements and provides guidance on:

- capturing of facial images to be used for verification or identification purposes in applications based on reference images in identity or similar documents and traveller or visa databases;
- capturing of fingerprint images to be used for verification or identification purposes in applications based on reference images in identity or similar documents and traveller or visa databases;
- data quality maintenance for biometric data captured by/for verification or identification applications;
- data authenticity maintenance for biometric data captured by/for verification or identification applications.

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

- biometric data quality and interoperability assurance;
- data authenticity assurance;
- morphing and other presentation attacks and biometric data injection attacks;
- accessibility and usability;
- recognition algorithms and their evaluation;
- privacy and data protection;
- optimal process design.

The following aspects are out of scope:

- other aspects of IT security;
- data capturing for ID document enrolment purposes, e.g. passport or ID card enrolment.

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 2382-37:2022, *Information technology - Vocabulary - Part 37: Biometrics*

ISO/IEC 29794-4, *Information technology - Biometric sample quality – Part 4: Finger image data*

ISO/IEC 29794-5, *Information technology - Biometric sample quality – Part 5: Face image data*

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

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

3 Terms and definitions

For the purpose 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 https://www.electropedia.org/
- ISO Online Browsing Platform available at http://www.iso.org/obp.

3.1
automated border control system
ABC
automated system which authenticates the electronic machine readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records, then determines eligibility of border crossing according to the pre-defined rules

3.2
biometric capture
collecting or attempting to collect a signal(s) from a biometric characteristic(s), or a representation(s) of a biometric characteristic(s,) and converting the signal(s) to a captured biometric sample set

3.3
border guard
public official assigned, in accordance with national law, to a border crossing point or along the border or the immediate vicinity of that border who carries out, in accordance with the Schengen Borders Code and national law, border control tasks

[SOURCE: Regulation (EU) No. 2016/399 [2]]

3.4
database
application storing a structured set of data and allowing for the management and retrieval of such data

EXAMPLE: The Schengen Information System (SIS) is a joint information system that enables the competent authorities in each Member State of the Schengen area, by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks carried out within the country in accordance with national law and, for some specific categories of alerts (those defined in Article 96 of the Schengen Convention), for the purposes of issuing visas, residence permits and the administration of legislation on aliens in the context of the application of the provisions of the Schengen Convention relating to the movement of persons

3.5
data subject
identified or identifiable natural person

Note 1 to entry: Depending on the context, the definition from ISO/IEC 2382-37:2022 can also be appropriate: individual whose individualized biometric data is within the biometric system.

[SOURCE: GDPR Art. 4(1) [3]]

3.6
digital mirror
display showing the horizontally mirrored live image of the camera's capturing area

3.7
face region
rectangle containing the central region of interest of a face visible in the face image

Note 1 to entry: The face bounding box is used for the estimation of landmarks to restrict the face image to the region of interest.

3.8
eID
electronically enabled card that may be used as an identity document

3.9
ePassport
machine readable passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, one or more biometric samples of the passport holder, and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology

3.10
machine readable zone
MRZ
area on a MRTD containing two lines of data (three lines on a TD-1 card) that are printed using a standard format and font to allow machine reading using optical character recognition methods

Note 1 to entry: See also “visual inspection zone (VIZ)”.

3.11
Member State
country which is a member of the European Union

Note 1 to entry: Within the context of the present recommendations, the term also applies to those countries that, not being EU members, take part in the Schengen area. See also “Schengen area”.

3.12
MRTD
official document issued by a state or organization and used by the holder for international travel, and containing mandatory visual data and a separate mandatory data summary in a format that is capable of being read by machine

EXAMPLE: machine readable passport, machine readable visa, machine readable official travel document

3.13
presentation attack
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

3.14
Schengen Area
area comprising European countries that have officially abolished border control at their mutual borders

Note 1 to entry: Currently, the Schengen area comprises all EU Member States except Cyprus and Ireland and four non-EU countries, namely Iceland, Liechtenstein, Norway and Switzerland

Note 2 to entry: The Schengen area takes its name from the Schengen Agreement signed in Schengen, Luxembourg, in 1985; this agreement was later incorporated into the EU legal framework by the 1997 Treaty of Amsterdam.

3.15
visual inspection zone
VIZ
portion of the MRTD (data page in the case of an ePassport) designed for visual inspection, i.e. front and back (where applicable), not defined as the MRZ

Note 1 to entry: See also “Machine Readable Zone (MRZ)”.

3.16
watch list
list of individuals, groups, or items that require close surveillance

4 Abbreviated terms

ABC	automatic border control
CEN	European Committee for Standardization
DET	detection error tradeoff
DG2	Data Group 2 (eMRTD face image)
DG3	Data Group 3 (eMRTD fingerprint image)
EEA	European Economic Area
eMRTD	electronic MRTD
EU	European Union
EU/EEA/CH	European Union/European Economic Area/Switzerland
FAR	false accept rate
FRR	false reject rate
FMR	false match rate
FNMR	false non-match rate
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organization
IR	infrared
ISO	International Organization for Standardization
KYC	know your customer
MRTD	machine-readable travel document
MRZ	machine readable zone
RFID	radio frequency identification
SC	subcommittee
SDK	software development kit
TC	technical committee
TS	technical specification
UMF	universal message format

VIS	visa information system
VIZ	visual inspection zone
WG	working group

5 Overview of biometric recognition systems

5.1 Concept

Depending on the context, biometric recognition can be performed manually or automatically.

There are several contexts in which biometric recognition is used. Typical use case covered in this document are border crossings, both with manual or automated controls, police inspections or contexts where governmental services play a role.

An automated biometric recognition system solution checks the authenticity of the travel document presented by a capture subject and the capture subject's ownership of that document using their biometric data. An eMRTD based system may make use of all the biometric modalities recommended by ICAO, for example face or finger. While other biometric modalities could be used for recognition, this TS concentrates on the ones approved by ICAO [5].

As automated systems can also be based on another token than an eMRTD or can be tokenless, the authenticity check of the identity document may be done at the time of enrolment for the system.

An important issue concerns the need for clearly defined protocols when failures appear in a fully automatic system (without human supervision). Failures can lead to false rejection of bona-fide users or problems with outliers (i.e. people that have difficulty in fully showing their face due to cultural reasons). In such situations, and to avoid raising acceptance issues, an alternative procedure is needed. Such an alternative procedure can consist of performing identity verification with a dedicated capture system with assistance from a human operator.

5.2 Biometric references

The use of biometric data is key for ensuring a close binding between the person and the document.

As described in [6] two general types of recognition systems can be identified in relation to their use of biometric references, token-based or tokenless, which generally applies to recognition systems:

- Token based systems require the capture subject to present a token (eMRTD, MRTD, ID card or any other issued or approved token) to the system, to provide additional authentication information or biometric references.

- If local legislation does not require the presentation of an identity document for being checked, it is possible to rely only on live biometrics capture of pre-enrolled qualified (vetted) capture subjects at the time of inspection. In this case immediate (1:N) comparison against an up-to-date list of authorized capture subjects would take place without any document inspection during the recognition process. Legislation might require that capture subjects carry a valid identity document even if this document does not have to be presented for inspection.

This document focuses on the biometric aspect of both types of systems.

5.3 Types of identity documents

5.3.1 General

Usually, capture subjects wishing to enter the European Union are required to carry a passport as a travel document compliant with the ICAO Doc 9303 attesting the holders' nationality and their biographic data.