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.

This Technical Specification was corrected and reissued by the CEN-CENELEC Management Centre on 9 February 2022.

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.