SLOVENSKI STANDARD
kSIST-TP FprCEN/TR 18108:2024

01-julij-2024

Osebna identifikacija - Uporaba biometričnih podatkov v izvornih dokumentih

Personal identification - Usage of biometrics in breeder documents

Personenidentifizierung - Verwendung biometrischer Daten in Hoheitsdokumenten

Ta slovenski standard je istoveten z: **FprCEN/TR 18108**

ICS:

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

kSIST-TP FprCEN/TR 18108:2024 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER REPORT

FINAL DRAFT
FprCEN/TR 18108

April 2024

ICS

English Version

Personal identification - Usage of biometrics in breeder documents

Personenidentifizierung - Verwendung biometrischer Daten in Hoheitsdokumenten

This draft Technical Report 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 Report. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Report.

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/TR 18108:2024 E

Contents

Page

European foreword

This document (FprCEN/TR 18108:2024) 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.

This document is currently submitted to the Vote on TR.

Introduction

Birth certificates and marriage certificates are collectively referred to as breeder documents. Obtaining authentic travel documents based on false breeder documents poses a major threat. The CEN/TS 17489 series [1] provides guidance on secure and interoperable European breeder documents that can be used for establishing and verifying identity in various scenarios such as application for ePassports and other identity documents.

A secure binding of breeder documents to their legitimate holders would increase the trust in the breeder documents and prevent identity theft. This can be achieved using biometrics, but several challenges arise in the context of breeder documents: In the case of birth certificates, the acquisition of biometric characteristics from infants can be impractical. Furthermore, as some biometric characteristics are sensible to ageing, linking breeder documents to their legitimate holders can become difficult after some time.

This document discusses options for the use of biometrics in breeder documents. It compares fingerprint, face, iris, palmprint, footprint, palm vein and finger vein recognition regarding verification performance, privacy impact, feasibility of biometric acquisition in different age groups and permanence of biometric features. Though resistance against presentation attacks (spoofing) is also required, a comparison regarding presentation attack resistance is omitted because these biometric modes can fulfil this criterion to a similar extent. Several studies have presented ways in which biometric characteristics can be forged. Presentation attack detection is possible but can increase the FNMR.

Even though non-coding DNA profiles allow a reliable verification of identity over the entire lifetime, DNA profiles are not taken into consideration for use in breeder documents. The reason is that processing of genetic material poses prohibitive risks to the rights and freedoms of natural persons because it can give rise to discrimination as it can reveal ethnic origin or genetic diseases [2].

1 Scope

This document provides guidance on usage of biometrics in breeder documents, in particular regarding

— encoding of biometric reference data,

— data quality maintenance for biometric reference data,

— data authenticity maintenance for biometric reference data, and

— privacy preservation of biometric reference data.

This document addresses advantages and disadvantages of biometric modes, in particular regarding

— verification performance,

— privacy impact,

— feasibility of biometric acquisition considering the age of the capture subjects,

— limits of validity and need for updating biometric reference data.

The following aspects are out of scope:

— format and structure of breeder documents,

— general security aspects, which are covered in CEN/TS 17489-1 [1].

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 [3] 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
biometric characteristic
biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition

[SOURCE: ISO/IEC 2382-37:2022 [3], 37.01.02]

3.2
biometric data
biometric sample or aggregation of biometric samples at any stage of processing

[SOURCE: ISO/IEC 2382-37:2022 [3], 37.03.06]

3.3
biometric mode
combination of a biometric characteristic type, a sensor type and a processing method

[SOURCE: ISO/IEC 2382-37:2022 [3], 37.02.05]

3.4
breeder document
foundational document
evidentiary document issued as a physical token of an event or status for a person and used by issuing authorities to establish identity and confirm entitlement

EXAMPLE Breeder documents include birth certificates and marriage certificates.

[SOURCE: ICAO TRIP Guide on evidence of identity [4]]

4 Abbreviated terms

DNA	deoxyribonucleic acid
FMR	false match rate
FNMR	false non-match rate
MRTD	machine-readable travel document

5 General set-up

According to CEN/TS 17489-1 [1], breeder document data must be digitally signed to ensure the integrity and authenticity of the data. The digital signature can be verified using a public key infrastructure (PKI). The signature verification can be performed offline (provided that all data required for the signature verification, i.e. public-key certificates and certificate revocation lists, are available) or online (server-based).

The CEN/TS 17489 series [1] distinguishes between

— Paper-based breeder documents, on which the breeder document data are printed in a human-readable format as well as in form of machine-readable two-dimensional (2D) bar codes,

— Hardware-based breeder documents, which provide the breeder document data in a machine-readable format on an integrated circuit, also called chip, and

— Server-based breeder documents, for which the digital signature is stored on the server.

A 2D bar code provides only limited storage space (about 3 kByte). The storage space on a chip and on a server is much less restricted.

A digital signature has a limited validity period. After expiration of the validity period, the digital signature cannot be used any longer to ensure the integrity and authenticity of the breeder document data. Therefore, the breeder documents have to be re-issued after expiration of the validity period unless the digital signature is stored and renewed on a server.

Threats to breeder documents include that someone else than the legitimate holder uses a genuine breeder document to establish identity or confirm entitlement. To enable reliable identity verification, biometric reference data of the document holder can be stored on the breeder document or on a trusted and certified European server [5].

6 Constraints on biometric data for reliable identity verification

This clause summarizes external constraints that do not originate from this document. To be suitable for verifying the identity of the holder of a breeder document, biometric characteristics must fulfil the following requirements:

— The biometric data must be adequate and limited to what is necessary for verifying the identity of the document holder.

— It must be easy to acquire biometric samples of sufficient quality at the time of breeder document issuance and at the time of breeder document verification.

— The biometric characteristics must be invariant over a sufficiently long time.

A system that employs biometrics for reliable identity verification of breeder-document holders must meet requirements and recommendations defined outside this document, among others:

— Starting from a trusted enrolment system, the integrity and authenticity of the biometric reference data must be ensured.

— Access to the biometric reference data must be controlled, and their confidentiality must be protected during transmission.

— It must be possible to distinguish between bona-fide presentations and presentation attacks or data injection attacks or morphing attacks.

— The biometric reference data must be technically usable by other suppliers' subsystems.

7 Suitability assessment of biometric modes for use on breeder documents

7.1 Fingerprint

7.1.1 Verification performance

In case of two-finger comparisons and an adult population, the most accurate fingerprint comparison systems using standardized finger minutiae templates yield an FNMR of 0,15 % (about 1 in 667) at an FMR of 0,1 % (1 in 1000) [6]. The most accurate fingerprint comparison systems using proprietary templates achieve an FNMR of 0,06 % (about 1 in 1667) at an FMR of 0,1 % (1 in 1000) in case of two-finger comparisons and an adult population [7].

Babies' fingerprints do not allow reliable verification of identity [8][9][10]. Fusing the comparison results of baby thumb and index fingers significantly improves the verification performance [11].

A reliable verification of identity of children aged between 6 years and 12 years is achievable if the finger image quality is adequate [12].

7.1.2 Privacy considerations

Fingerprints are considered more sensitive personal information than face images. Therefore, access to fingerprints is to be protected using additional cryptographic access control mechanisms when stored in MRTDs [13].

Storing biometric templates containing extracted feature data instead of raw image data does not strongly protect the privacy of the stored biometric data as, in case of data leakage, a matching synthetic sample can be reconstructed from an unprotected template [14].

7.1.3 Collectability

Several feasibility studies concluded that fingerprinting babies is virtually impossible using ordinary (500 pixels per inch) fingerprint scanners [15][16][17]. A high-resolution sensor with a spatial sampling rate of at least 1000 pixels per inch is required for capturing babies' fingerprints of sufficient quality [8][9].

7.1.4 Template aging

Fingerprint growth can be modelled using an isotropic growth model, and recognition performance of fingerprint systems can be improved by scaling up the fingerprint images using this model when comparing fingerprints of adolescents collected over time [18].

There is no widespread fingerprint ageing effect in adult populations [19][20].

7.1.5 Interoperability issues

To be usable by other suppliers' subsystems, the biometric reference data must be stored in a standardized format. MRTDs are required to carry image data in a standardized data interchange format ([21][22]) because image data can offer a higher level of interoperability in multi-vendor systems than processed feature data do [6]. JPEG 2000 [23] compression of 500 dpi (196,85 pixels per centimetre) finger images of size 300 × 300 pixels yields file sizes of 4,4 kB while causing only a negligible decrease in verification performance [26].

Storing compact biometric templates containing extracted feature data rather than raw image data helps in accelerating biometric recognition, reducing the memory consumption, and enhancing the privacy in terms of lower information leakage. The most widely used fingerprint feature data are finger minutiae, for which data interchange formats have been standardized [23][25] and an acceptable interoperability performance can be achieved [6]. The tagged binary finger minutiae data format contains 5 bytes per minutia. Thus, the size of the main body of a finger minutiae data block containing 60 minutiae (which is the recommended maximum number of minutiae for on-card comparison [23]) is 300 bytes.

7.2 Face

7.2.1 Verification performance

At the time of writing, for mugshots of adult subjects, the most accurate face comparison systems yield an FNMR of 0,21 % (about 1 in 475) at an FMR of 0,000 1 % (1 in 1 000 000) [27].

Baby face images do not allow reliable verification of identity [28][29][30][31].

7.2.2 Privacy considerations

Face images do not disclose information that the capture subject does not routinely disclose to the general public. Face verification against reference images stored in paper-based or hardware-based breeder documents has little privacy impact.

Remote mass storage of reference face images entails a higher risk of function creep. Even if currently unlawful, reference face images stored on a server for the purpose of reliable identity verification could later be misused for the purpose of biometric identification of anyone in the database.

7.2.3 Collectability

Because children can exhibit different poses and expressions while being photographed, it is very difficult to capture good-quality face images from children [32][33]. For example, capture of fully ICAO-compliant face images for children's passports is attempted only starting from the age of 10 years.