SLOVENSKI STANDARD
SIST-TS CEN/TS 17261:2019

01-februar-2019

Biometrična avtentikacija za nadzor kritične infrastrukture - Zahteve in ovrednotenje

Biometric authentication for critical infrastructure access control - Requirements and Evaluation

Biometrische Authentifikation für die Zugangskontrolle zu kritischen Infrastrukturen - Anforderungen und Evaluierung

Authentification biométrique pour le contrôle d'accès aux infrastructures critiques - Exigences et évaluation

Ta slovenski standard je istoveten z: **CEN/TS 17261:2018**

ICS:

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

SIST-TS CEN/TS 17261:2019 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 17261

December 2018

ICS 35.240.15

English Version

Biometric authentication for critical infrastructure access control - Requirements and Evaluation

Authentification biométrique pour le contrôle d'accès aux infrastructures critiques - Exigences et évaluation

Biometrische Authentifikation für die Zugangskontrolle zu kritischen Infrastrukturen - Anforderungen und Evaluierung

This Technical Specification (CEN/TS) was approved by CEN on 10 September 2018 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, 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 17261:2018 E

Contents

Page

European foreword

This document (CEN/TS 17261:2018) 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.

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

Introduction

This document is concerned with the performance-based testing of biometric authentication for automated access control systems (AACS), in particular for physical access control to controlled areas of Critical Infrastructure as defined by the European Council Directive 2008/114/EC [7].

It is assumed that biometric recognition constitutes a second authentication factor alongside token-based authentication and that the AACS requires the results of the biometric and token-based authentication of the same individual before authorizing access. The biometric+token combination emulates a biometric verification system. The token presentation constitutes the biometric claim that the capture subject is the bodily source of the biometric reference associated with the token ID. Accordingly, technical performance of the biometric authentication is assessed in terms of verification metrics, i.e. False Accept Rate, False Reject Rate, Failure-to-Enrol Rate and throughput rates. Technical performance requirements and evaluation methods should be identical irrespective of the biometric technology.

Biometric subsystems should also be evaluated in terms of their vulnerability to defeat. This is to be assessed through measuring a system's capacity to resist a direct attack on it or detect an intrusion attempt by a knowledgeable attacker intent on defeating the biometric authentication. Since method of attack is dependent on the biometric technology, vulnerability to defeat is assessed in a technology-specific manner.

The results of an evaluation performed using this document relate to the system's performance in that the evaluation should not be used as a guarantee of the performance that would be expected on any other site.

1 Scope

This document addresses biometric recognition systems that are used as part of an automated access control system to provide a second and independent authentication factor of the individual using the AACS to access secured areas of critical infrastructure.

This document:

— specifies requirements for biometric recognition systems to be used as part of an AACS for critical infrastructure,

— describes a methodology for the evaluation of biometric authentication for AACSs against the specified requirements.

The requirements and test methods address biometric authentication for AACS that: (i) operate in an internal environment constituting part of a larger site, access to which is restricted and controlled by a separate access control system; and (ii) use biometrics as a second authentication factor to a token or proximity card.

This document does not consider access by the general public, e.g. passengers in an airport, or visitors to a hospital.

Products that meet the requirements of this document will comprise (i) a biometric sensor(s) external to the secured area, which reads the biometric characteristics of the user at the point of access; and (ii) a biometric server system performing biometric enrolment, signal processing, storage of biometric references and biometric comparison within a secured area.

This document does not address AACS or AACS portals (turnstiles) but is only concerned with the biometric components which integrate with the AACS. Other standards address requirements and testing of the non-biometric parts of the AACS.

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, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 30107-3:2017, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in 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 http://www.electropedia.org/

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

3.1
attack potential
measure of the effort to be expended in attacking a target of evaluation (TOE), expressed in terms of an attacker's expertise, resources and motivation

[Source: ISO/IEC 15408-1:2009]

3.2
critical infrastructure
asset, system or a part thereof that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions

3.3
enrolment transaction duration
measurement of the duration of an enrolment transaction, starting when the enroller begins a interaction with the biometric enrolment system to conduct the enrolment (e.g., authenticating as a valid enroller on the system) and ending when the enrolee's biometric reference is stored in the system, or when a failure-to-enrol is declared

3.4
evaluation laboratory
organisation that carries out the evaluation

3.5
false accept rate
FAR
proportion of non-mated verification transactions erroneously confirmed

[SOURCE: ISO/IEC 19795-1:2006, modified to harmonise with the vocabulary of ISO/IEC 2382-37]

3.6
false reject rate
FRR
proportion of mated verification transactions erroneously rejected

[SOURCE: ISO/IEC 19795-1:2006, modified to harmonise with the vocabulary of ISO/IEC 2382-37]

Note 1 to entry: Rejections due to failure-to-acquire errors or to false alarms in spoof detection are included in the false reject rate.

3.7
generalized false reject rate
GFRR
generalization of the false reject rate that includes the effect of enrolment failures: the test participants who the system failed to enrol are considered to have made verification transactions equivalent to those of enrolled test subjects, and these verification transactions are considered to have failed

3.8
habituated capture subject
biometric subject familiar with using the biometric device

Note 1 to entry: Transaction times and success rates for habituated test subjects will be consistent with those experienced in their regular use of the system.

3.9
impostor attack presentation match rate
IAPMR
proportion of impostor attack presentations, using the same attack method, in which the target reference is matched

[SOURCE: ISO/IEC 30107-3:2017 (“PAI species” changed to “attack method”)]

3.10
mated verification transaction

verification transaction in which the accompanying token (i.e., biometric claim) corresponds to the capture subject

Note 1 to entry: Mated verification transactions have historically been called genuine transactions.

3.11
non-mated verification transaction
verification transaction in which the accompanying token (i.e., biometric claim) does not correspond to the capture subject

Note 1 to entry: Non-mated verification transactions have historically been called (zero-effort) “impostor” transactions.

3.12
presentation attack
presentation to the biometric capture subsystem with the goal of interfering with the correct operation of the biometric system

Note 1 to entry: In the context of this document, the goal of a *presentation attack* is impersonation of another enrolled individual. A presentation attack can be implemented through a variety of methods, e.g. artefact, mutilation, replay, etc.

3.13
verification transaction duration
measurement of the duration of a verification transaction, starting when the subject begins interaction with the biometric capture device and ending when the biometric system renders a final transaction decision

3.14
secured area
area or facility to which access is restricted to authorised roles under the security policy

EXAMPLE Data centres, communication rooms, command and control facilities.

Note 1 to entry: In this document, secured areas do not include areas accessible to the general public, e.g. passengers in an airport, or visitors to a hospital.

3.15
supplier
organisation or person that provides the product under evaluation and provides support during the evaluation term

4 Symbols and abbreviations

For the purposes of this document, the following abbreviations apply.

AACS	Automated Access Control System
FAR	False Accept Rate
FRR	False Reject Rate
FTER	Failure to Enrol Rate
GFRR	Generalized False Reject Rate
IAPMR	Impostor Attack Presentation Match Rate
IAPMR$_{BASIC}$	Maximum value of IAPMR over all tested attack methods at attack potential BASIC or below

5 Conformance

A biometric subsystem integrated into an AACS conforms to the specifications of this document if:

a) it meets all requirements contained in 7.2,

b) the performance and attack resistance metrics specified in Table 1 have been tested and reported in accordance with the requirements of 7.4, 7.5 and Clause 8 and

c) the performance and attack resistance meets the baseline performance levels specified in 7.6, Table 1.

6 Typical use-case

This document addresses Automated Access Control Systems operating in an internal environment constituting part of a larger site, where biometric authentication is used as a second authentication factor working independently of authentication by token or proximity card.

Authorized individuals are issued with tokens for use by the AACS and are also enrolled into the biometric system.

The biometric enrolment records the biometric characteristics of an individual and generates a biometric reference against which future comparisons can be made. This reference is stored together with the system identifier for that individual. The organization's Security Policy will specify the credentials that

an individual needs to provide to show eligibility for biometric enrolment. The Security Policy may also allow for re-enrolment to update an individual's biometric reference when required.

Access control tokens/cards together with biometric recognition will be required to allow entrance to (or exit from) the secured area(s).

7 Requirements and recommendations

7.1 General

Requirements and recommendations for the biometric authentication subsystem are divided into requirements and recommendations regarding:

— the design,

— the operation,

— the performance and

— the attack resistance.

7.2 Design

7.2.1 General

The biometric system shall provide functionality to support the design requirements given in 7.2.2 to 7.2.6.

7.2.2 Protection of access to biometric server, biometric data and functions of the biometric subsystem

The biometric server shall be located within a secured area. To avoid the need to evaluate against the possibility of cyberattack, the server shall have no data connections outside the secured area other than to biometric door units, (e.g. Wi-Fi connection between components or cloud storage of biometric references and transactions logs are prohibited).

To maintain independence between token and biometric authentication, the biometric reference shall not be stored on the token.

7.2.3 Operator/Administrator control and authentication

Operator/administration functions shall take place on the biometric server system and shall not be available on the biometric door units external to the secured area.

The system shall be configured to verify the identity and the authority of staff operating the system (e.g. system administrator, enroller) immediately prior to:

— biometric enrolment or re-enrolment,

— the deletion of biometric references,

— backup and restoration of the biometric database,

— configuration of system parameters (e.g. comparison score thresholds, presentation attack detection settings, etc.) for the biometric component and

— the inspection of results logged by the system.