PD CEN/TS 17261:2018

BSI Standards Publication

Biometric authentication for critical infrastructure access control - Requirements and Evaluation

bsi.

National foreword

This Published Document is the UK implementation of CEN/TS 17261:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/44, Biometrics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2018

ISBN 978 0 580 99910 9

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 December 2018.

Amendments/corrigenda issued since publication

Date	Text affected

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: Avenue Marnix 17, B-1000 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]