

STN P	Identifikácia osôb Odolnosť voči útoku napodobňovaním biometrie Použitie na automatickú kontrolu európskych hraníc	STN P CEN/TS 17262 36 9754
------------------	---	--

Personal identification - Robustness against biometric presentation attacks - Application to European Automated Border Control

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 03/19

Táto predbežná STN je určená na overenie. Pripomienky zasielajte ÚNMS SR najneskôr do 31.12.2020

Obsahuje: CEN/TS 17262:2018

128229

TECHNICAL SPECIFICATION

CEN/TS 17262

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

December 2018

ICS 35.240.20

English Version

Personal identification - Robustness against biometric presentation attacks - Application to European Automated Border Control

Identification personnelle - Recommandations pour garantir la robustesse de la biométrie dans les systèmes de contrôle frontalier automatisés européens contre les attaques de présentation

Persönliche Identifikation - Empfehlungen zur Sicherung der biometrischen Belastbarkeit Europäischer ABC-Systeme gegenüber Manipulation

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

Contents

European foreword.....	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 Abbreviated terms.....	7
5 Presentation attack detection overview in ABC system	8
5.1 Obstacles to presentation attacks in ABC system.....	8
5.2 Impostor attacks.....	8
5.2.1 General.....	8
5.2.2 Verification of an eMRTD credential.....	8
5.2.3 Identification in a Registered Traveller Programme use case	9
5.2.4 Concealer attacks	9
5.3 Level of attack potential to consider.....	9
6 Minimal accuracy requirements guideline for ABC systems.....	10
7 PAD evaluation in ABC systems	10
7.1 Overview	10
7.2 Artefacts Properties	10
7.2.1 Overview	10
7.2.2 Artefacts for facial biometrics.....	10
7.2.3 Artefacts for fingerprint biometrics.....	11
7.3 Artefact creation and usage.....	12
7.4 Metrics for the evaluation of ABC systems.....	13
7.4.1 General metrics.....	13
7.4.2 Metrics for an impostor attack scenario with eMRTD credentials	14
7.4.3 Metrics for an impostor attack scenario in Registered Traveller Programme	14
7.4.4 Metrics for concealer attack scenario.....	14
7.4.5 Considerations on statistical relevance	14
8 Logging, data protection and privacy	14
9 Usability and the environment.....	15
Annex A (informative) Examples of attack potential ratings.....	16
A.1 General.....	16
A.2 Framework for the calculation of attack potential	16
A.3 Considerations for rating factors in ABC systems	18
A.3.1 Overview	18
A.3.2 Elapsed time.....	18
A.3.3 Window of opportunity: Access to the TOE	18
A.3.4 Window of opportunity: Access to biometric characteristics.....	19

A.4	Examples of application to ABC systems.....	19
A.4.1	Overview.....	19
A.4.2	Impostor Attack against a face-based ABC system in an eMRTD credential verification scenario.....	19
A.4.3	Impostor Attack against a fingerprint-based ABC system for Identification in a Registered Traveller Programme scenario.....	20
A.4.4	Concealer Attack against a watchlist in an ABC system.....	21
	Bibliography	23

CEN/TS 17262:2018 (E)**European foreword**

This document (CEN/TS 17262:2018) 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.

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

EU Member States issue electronic passports (ePassports) containing a smart-card chip that stores biometric data. The biometric data stored is a face image and two finger images of the holder, except for Ireland and the UK, which issue ePassports containing only a face image. A number of EU Member States have deployed automated border control (ABC) systems that automate border checks for EU citizens in possession of an ePassport. An ABC system authenticates the ePassport, verifies that the traveller is the rightful holder of the ePassport by comparing presented biometric characteristics with biometric data stored in the ePassport, queries border control records (possibly involving biometric identification of the traveller in watchlists), and finally determines eligibility of border crossing according to pre-defined rules, without intervention of a border guard. Border guards can supervise several ABC lanes and intervene whenever something does not work as expected or the traveller hits a watchlist.

Even though supervised, ABC systems are potentially vulnerable to biometric presentation attacks. A biometric presentation attack (or spoofing) is the presentation of artefacts or human characteristics to the biometric capture subsystem in a fashion that may interfere with the system policy. Techniques for the automated detection of presentation attacks are called presentation attack detection (PAD) mechanisms.

This document deals with best practice recommendations regarding the PAD capabilities of European ABC systems.

CEN/TS 17262:2018 (E)

1 Scope

This document is an application profile for the International Standard ISO/IEC 30107. It provides requirements and recommendations for the implementation of Automated Border Control (ABC) systems in Europe with Presentation Attack Detection (PAD) capability.

This document covers the evaluation of countermeasures from the Biometrics perspective as well as privacy, data protection and usability aspects. Technical descriptions of countermeasures are out of scope. Enrolment, issuance and verification applications of electronic Machine Readable Travel Documents (eMRTD) other than border control are not in scope. In particular, presentation attacks at enrolment are out of scope.

The biometric reference data can be stored in an eMRTD and/or in a database of registered travellers.

This document covers:

- biometric impostor attacks and
- biometric concealer attacks in a watchlist scenario.

This document addresses PAD for facial and fingerprint biometrics only.

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 (series), *Information Technology — Biometric presentation attack detection*

CEN/TS 16634, *Personal identification - Recommendations for using biometrics in European Automated Border Control*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN