SLOVENSKI STANDARD
SIST-TS CEN/TS 17262:2019

01-februar-2019

Osebna identifikacija - Odpornost proti napadom na biometrično predstavitev - Uporaba pri evropskem avtomatiziranem mejnem nadzoru

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

Persönliche Identification - Empfehlungen zur Sicherung der biometrischen Belastbarkeit Europäischer ABC-Systeme gegenüber Manipulationen

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

Ta slovenski standard je istoveten z: **CEN/TS 17262:2018**

ICS:

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

SIST-TS CEN/TS 17262:2019 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 17262

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

Ref. No. CEN/TS 17262:2018 E

Contents

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.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, CEN/TS 16634, ISO/IEC 30107 (series) 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 http://www.iso.org/obp

3.1
automated border control system
ABC system
automated system which authenticates the electronic machine readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records and other relevant records or databases, then determines eligibility of border crossing according to the predefined rules

3.2
imposter attack presentation match rate BASIC
$IAPMR_{BASIC}$
in an evaluation of an ABC system in a verification scenario, maximum value of IAPMR obtained by a PAI species of attack potential BASIC among those evaluated

3.3
imposter attack presentation identification rate BASIC
$IAPIR_{BASIC}$
in an evaluation of an ABC system in an identification scenario, maximum value of IAPIR obtained by a PAI species of attack potential BASIC among those evaluated

3.4
concealer attack presentation non identification rate BASIC
$CAPNIR_{BASIC}$
in an evaluation of an ABC system in a watchlist identification scenario, maximum value of CAPNIR obtained by a PAI species of attack potential BASIC among those evaluated

4 Abbreviated terms

The abbreviated terms shown in Table 1 are used in this document.

Table 1 — Abbreviated Terms

Abbreviations	Terms
ABC	Automated Border Control
APCER	Attack Presentation Classification Error Rate
APMR	Attack Presentation Match Rate
APNRR	Attack Presentation Non-Response Rate
BPCER	Bona Fide Presentation Classification Error Rate
BPNRR	Bona Fide Presentation Non-Response Rate
CEN	European Committee for Standardization
CAPNIR	Concealer Attack Presentation Non-Identification Rate
$CAPNIR_{BASIC}$	Concealer Attack Presentation Non-Identification Rate BASIC
eMRTD	electronic Machine Readable Travel Document
EU	European Union
FTA	Failure to Acquire
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False Non Match Rate
FPIR	False Positive Identification Rate
FS-PD	Full System Processing Duration
GDPR	General Data Protection Regulation

Abbreviations	Terms
IAPIR	Imposter Attack Presentation Identification Rate
$IAPIR_{BASIC}$	Imposter Attack Presentation Identification Rate BASIC
IAPMR	Imposter Attack Presentation Match Rate
$IAPMR_{BASIC}$	Imposter Attack Presentation Match Rate BASIC
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PAD	Presentation Attack Detection
PAI	Presentation Attack Instrument
TOE	Target of Evaluation
TS	Technical Specification

5 Presentation attack detection overview in ABC system

5.1 Obstacles to presentation attacks in ABC system

By definition, biometric presentation to ABC systems is not directly supervised by an operator. An operator should be present but is typically monitoring several ABC systems at the same time. Intervention by the operator may be requested by the system if a fraud attempt is detected, or if the capture subject is identified against a watchlist, which are the outcomes an attacker wants to avoid. The operator will also become actively involved in a transaction if a capture subject fails to be recognized by the system after a certain number of attempts. In this case of multiple rejections, human intervention is needed to check the identity credential of the capture subject before processing through the border is allowed.

The absence of direct supervision means that attackers may use artefacts with only limited visual plausibility. Nevertheless, the presence of an operator nearby means the attacker could attract attention by using artefacts which are too voluminous (like fake heads for example) or using fraud techniques which take more time or more attempts than normally needed to cross ABC systems.

Abnormal or lengthy activities during presentation at ABC systems may also attract attention from other people crossing the ABC systems and raise alarm.

5.2 Impostor attacks

5.2.1 General

Biometric imposters aim to attack a system by impersonating the biometric characteristics of another person.

In order to be effective, the artefact is successfully matched and presentation attack detection does not raise any alarm.

5.2.2 Verification of an eMRTD credential

An attacker may have acquired an eMRTD credential and the corresponding biometric characteristics of the rightful user. The attacker will hence create an artefact mimicking these characteristics in order to be verified when presenting the artefact at the ABC system. While the attacker may have stolen the credential and used subterfuge to acquire the biometrics data (like latent fingerprint), it is also possible that the owner of the credential is an accomplice and has provided high-quality samples of fingerprints or the face.

5.2.3 Identification in a Registered Traveller Programme use case

In cases where biometric characteristics acquired in an ABC system are identified against a data set of authorized or registered travellers, the attacker may target a specific identity upon which they have acquired the characteristics. Alternatively, the attacker may also target any registered identity in the data set by using an artefact with high false positive identification probability.

The attacker may also try to re-activate remaining latent fingerprints on the sensor left by the previous legitimate user.

5.2.4 Concealer attacks

Biometric concealers aim to attack a system by hiding their biometric characteristics. The purpose is not to be matched against a biometric watchlist or similar system. The eMRTD used by the concealer attacker is not related to their true identity. The attacker also seeks to not attract unwanted attention from personnel by triggering, for example, multiple "Failure To Acquire (FTA)" signals, so the artefact might have characteristics likely to be confused with genuine biometric characteristics. In order to be successful, the artefact does not raise any alarm from presentation attack detection. In the context of ABC systems, the goal of an attacker is not to be recognized but still to be able to cross the border. The attacker has two ways to achieve this:

1. The attacker may try to exploit the system policy for managing unsuccessful biometric verification. Typically, after a given number of failed attempts fixed by the system policy, an ABC system user will be redirected to a human officer for manual check.

   NOTE This document only addresses the presentation of biometric characteristics to a sensor, the fallback processes that could be implemented by the system policy after a failure are out of scope.

   EXAMPLE As only one officer typically monitors several ABC systems, the manual check after an ABC system rejection could be less adequate than a regular manual check in case of overcrowded border. Therefore, the attacker could rely on forged identity credentials to proceed through the border after having been rejected by automated access.

2. Alternatively, the concealer attack could be accompanied by an impostor attack where the attacker tries to match the biometric data stored in the eMRTD with that of another identity.

5.3 Level of attack potential to consider

ISO/IEC 30107-3 and ISO/IEC 19989 ([1], currently under development by ISO/IEC JTC 1/SC 27) refer to the Common Criteria terminology to evaluate the potential of presentation attacks. Attack potential can be rated as being "Basic", "Enhanced-Basic", "Moderate", "High" or "Beyond-High". Examples of Attack Potential Ratings can be found in Annex A. The level of attack potential considered for an evaluation is a major factor as it will determine what kind of attacks the system is supposed to be resilient to.

The attack potential rating is influenced by the level of knowledge available to an attacker on the system. To reduce an ABC system's vulnerability, technical details available publicly about the PAD method used should therefore be minimal. Ideally, ABC systems should not be available on the general public market to avoid easy access for attackers and limit the opportunity to test and elaborate specific attack methods.

Attack potential will be greatly influenced by the level of technological know-how required to produce artefacts. As information on most generic attack methodologies can be found quite easily in scientific papers or on websites by potential attackers, ABC systems should at least be resilient to attack methods requiring low or moderate technical means and ability.