



BSI Standards Publication

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

National foreword

This Published Document is the UK implementation of CEN/TS 17262:2018.

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.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 99911 6

ICS 35.240.20

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
------	---------------

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: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword	iii
Introduction	iv
1 Scope	5
2 Normative references	5
3 Terms and definitions	5
4 Abbreviated terms	6
5 Presentation attack detection overview in ABC system	7
5.1 Obstacles to presentation attacks in ABC system	7
5.2 Impostor attacks	7
5.2.1 General	7
5.2.2 Verification of an eMRTD credential	7
5.2.3 Identification in a Registered Traveller Programme use case	7
5.2.4 Concealer attacks	7
5.3 Level of attack potential to consider	8
6 Minimal accuracy requirements guideline for ABC systems	8
7 PAD evaluation in ABC systems	9
7.1 Overview	9
7.2 Artefacts Properties	9
7.2.1 Overview	9
7.2.2 Artefacts for facial biometrics	9
7.2.3 Artefacts for fingerprint biometrics	10
7.3 Artefact creation and usage	11
7.4 Metrics for the evaluation of ABC systems	12
7.4.1 General metrics	12
7.4.2 Metrics for an impostor attack scenario with eMRTD credentials	12
7.4.3 Metrics for an impostor attack scenario in Registered Traveller Programme	12
7.4.4 Metrics for concealer attack scenario	13
7.4.5 Considerations on statistical relevance	13
8 Logging, data protection and privacy	13
9 Usability and the environment	14
Annex A (informative) Examples of attack potential ratings	15
Bibliography	22

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

impostor 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