SLOVENSKI STANDARD
SIST-TS CEN/TS 16921:2016

01-julij-2016

Osebna identifikacija - Omejitve in zakonski profili za uporabo pravnega pregona za mobilne biometrične identifikacijske sisteme

Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems

Personenidentifikation - Biometrische Anwendungsprofile für Ordnungskräfte und Grenzübergangsverantwortliche, die tragbare Identifizierungssysteme einsetzen

Ta slovenski standard je istoveten z: CEN/TS 16921:2016

ICS:

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

SIST-TS CEN/TS 16921:2016 en

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16921

March 2016

ICS 35.240.15

English Version

Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems

Personenidentifikation - Biometrische Anwendungsprofile für Ordnungskräfte und Grenzübergangsverantwortliche, die tragbare Identifizierungssysteme einsetzen

This Technical Specification (CEN/TS) was approved by CEN on 25 January 2016 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, 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 16921:2016 E

Contents

Page

European foreword

This document (CEN/TS 16921:2016) 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 organizations of the following countries are bound to announce this Technical Specification: 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Most countries around the world are provided with identification systems for law enforcement and border control. To be consistent in such deployments and processes, technical documents, guidelines and best practice recommendations are being developed by different groups. However, these documents are primarily focused on Automated Border Control (ABC) systems and the technical and operational issues to be considered when planning and deploying such systems in Europe. There is little guidance covering the circumstances in which identification is not done in a fixed point, or for other purposes that cover any law enforcement application besides fixed ABC. There is a need for guidance for the use of mobile or portable identification capabilities as such systems have special biometrics characteristics: calibration problems, uncontrolled environment, specific biometric security aspects, that have to be considered differently for fixed point solutions.

Law enforcement authorities can use mobile and especially hand-held systems to check person’s identity under numerous circumstances, on borders as identity check for border control purposes as well as inside the national borders for standard law enforcement purposes like suspect identity check, police check point control, police swoop, etc. In any of these applications, the mobile system may be able to use identity document, or if not present, to check person’s identity using his/her biometrics against date base (local or remote).

1 Scope

This Technical Specification primarily focuses on biometric aspects of portable verification and identification systems for law enforcement and border control authorities. The recommendations given here will balance the needs of security, ease of access and data protection.

ISO/IEC has published a series of standards dealing with biometric data coding, interfaces, performance tests as well as compliance tests. It is essential for interoperability that all these standards are applied in European deployments. However, ISO/IEC standards do not consider national or regional characteristics; in particular, they do not consider European Union privacy and data protection regulation as well as accessibility and usability requirements.

This Technical Specification extends the ISO standards by emphasizing specific European needs (for example EU data Protection Directive 95/46/EC and European databases access). The Technical Specification systematically discusses issues to be considered when planning, deploying and using portable identity verification systems and gives recommendations for those types of systems that are or will be in use in Europe.

Communication, infrastructure scalability, and security aspects other than those related to biometrics are not considered. This document also does not consider hardware and security requirements of biometric equipment and does not recommend general identification procedures.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
biometric verification (1:1)
process of confirming a biometric claim through biometric comparison

[SOURCE: ISO/IEC 2382-37]

2.2
biometric identification (1:N)
process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual

[SOURCE: ISO/IEC 2382-37]

2.3
transportable
system capable of being carried or moved about. Moving this system may require some specialized procedures

2.4
workstation
system that can be carried by one person from place to place (typically size = suitcase; weight < 15 kg). Usually, once the system is in place subject shall move to it

2.5
hand-held
system that can be operated by handling in one hand (typically size < 30 cm; weight < 1 kg). Usually, controller can move to subject with the system

3 Symbols and abbreviations

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

ABC	Automated Border Control
CEN	European Committee for Standardization
eMRTD	electronic Machine Readable Travel Documents
EU	European Union
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JTC	Joint Technical Committee
NIST	National Institute of Standards and Technology
RFID	Radio-frequency identification
TS	Technical Specification
VIS	Visa Information System
WG	Working Group

4 Portable identity verification systems

4.1 Introduction

A portable identity verification system for law enforcement applications allows performing the identity verification of a citizen in contexts such as a police road block, foot or car patrol, etc. by comparing (1:1) a biometric sample captured live using the portable system with a reference sample (stored in an electronic document or in a remote database) or by performing a 1:N search in a database. Different functionalities can be made available by the system, depending on the availability of an electronic document and remote alphanumeric or biometric databases.

If an electronic document, containing biometric fingerprint data is available (i.e. eMRTD or electronic National Identity document), the portable identity verification system allows to:

— perform a biometric verification (1:1) by comparing a biometric fingerprint sample captured live with the portable system with the reference sample stored in the electronic document. Once it is established that the citizen is the rightful holder of the document, national or international databases can then be searched to find out if the citizen is present in any relevant databases;

— if the verification does not return a positive match or if the law enforcement officer has doubts about the citizen identity, a biometric identification (1:N) can also be performed, by sending the captured biometric (fingerprint) sample to an AFIS system for matching, followed by a search in the alphanumeric databases using the identity returned by the AFIS system (that can be different from the one written in the document). If the document only contains a facial image (no fingerprints) or an iris, it is also possible to perform a search in a remote face or iris recognition system, if available.

If the citizen does not have an electronic document (or has no document at all) the portable identity verification system allows to:

— perform a biometric verification (1:1) by comparing a biometric fingerprint sample captured live with the portable system with a reference sample stored in a remote database and identified by using information such as a national unique identity number or code ‘(in the case where the citizen has a non-electronic document) It is possible to perform this kind of verification if a National Biometric registry exists in the country and if every citizen is assigned a national unique identity number or code. In case of a positive match, the information stored in the National Biometric registry can be returned to the user of the system. Additional national or international databases can then be searched to find out if the citizen is present in any relevant databases;

- perform a biometric identification (1:N) by capturing a biometric fingerprint sample with the portable system and sending it for matching to an AFIS system, where the 1:N search is performed. Additional national or international databases can then be searched to find out if the citizen is present in any relevant databases. If the system allows capturing a facial image or an iris, it is also possible to perform a search in a remote face or iris recognition system, if available.

NOTE In the case of EU eMRTD, the biometric authentication consists in capturing the live biometric data of the user – fingerprint, iris or facial image – and comparing it with the biometric information stored in the eMRTD chip. The fingerprint and iris data are protected, and the portable identification system accesses this information through EAC protocol, whereas SAC or BAC only protocol is sufficient to access the facial image.

4.2 Typology of portable identity verification systems

Mobile ID devices have been employed for a variety of applications where a stationary collection environment is not possible or easily attainable. Applications include:

- the officer on the street or at a checkpoint who needs to perform a quick check against biometric data stored in a card or to biometric databases and/or watch-lists;
- security at high profile, major public events, where fixed ID systems may not be practical or appropriate;
- issuance of a citation that requires registration of the biometric with the incident;
- verification of the identity of subjects at court appearances;
- access control for buildings, or Critical Infrastructure buildings;
- security involving prisoner transport and release tracking;
- immigration and border control;
- entitlement programs and job applications.

These applications and others are being accomplished with on-the-spot acquisitions of biometric data for comparison with samples stored in key databases or in ID cards.

NOTE In this document, the biometric data refers to fingerprint, face, vein or iris, biometrics stored in central databases and/or ID documents.

4.3 Portable identity verification systems in border control environment

A portable border control system “authenticates the eMRTD, establishes that the traveller is the rightful holder of the document, queries border control records, then automatically determines eligibility for border crossing according to pre-defined rules” [1]. The use of biometric data are the key for ensuring a close binding between the person and the document.

The elements in a portable identification system are basically the same that are present in a fixed ABC (biometrics, travel document verification, communications as described in CEN/TS 16634 [3]) but the environment is very different (in a mobile installation environment is almost completely uncontrolled