PD CEN/TS 16921:2016

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 16921:2016.

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 2016

ISBN 978 0 580 91181 1
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 30 April 2016.

Amendments/corrigenda issued since publication

Date	Text affected

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

[8]). Also portable identity verification systems require sensor calibration and maintenance to ensure a proper working condition. As a portable device may change from place to place, testing for scenario adaptation could be more important than in a static placement. These conditions have influence in the system architecture and in biometrics performance. At least, the selection of the biometric technology used, quality conditions and available technology to perform identification and communication can be defined and evaluated.

5 General recommendations for portable identity verification systems

5.1 Biometric modalities

European portable systems are designed for the use of fingerprints and facial images. Adaption of other modalities like iris and vein is possible. The aim is to check that the traveller presenting a travel document really is the person to whom this document was issued and thus verifies the person's right to enter the territory. A portable identity verification system is not limited to identity verification at the borders but can also be used for identity verification within the territory of the nation, both for EU citizens and 3rd country nationals. A portable system should also allow to perform biometric identification (1:N search).

5.2 Usability and accessibility

NOTE General guidance on these aspects is given in ISO/IEC/TR 24714-1 and CEN/TS 16634.

For portable identity verification systems usability should be extended to the specific operational conditions. For hand-held devices, the operator should be holding the device while biometric data are acquired from the subject (for example fingerprint, face). In this case, operator and user share the device and special considerations should be taken to allow an easy and ergonomic use.

Portable systems should be designed to be equitable in use for subjects who have permanent or temporary physical or psychological inabilities. They should be easy to use and with a wide tolerance of operation. For subjects that cannot use the biometric system alternative systems are necessary and should be provided.

Hand-held devices are small with limited user guidance display possibilities. Subjects need simple and clear instructions to present the fingerprint to the capture device. Therefore operators should be trained in order to guide the subjects.

The operator should get immediate feedback and guidance on how to get images of acceptable quality. This feedback can be displayed on the device in a way that it is not visible to the subject.

5.3 European data protection regulation

EU and national privacy and security legal requirements have to be met regardless of implementation issues such as local database storage.

5.4 Architecture

5.4.1 General aspects of architecture

The aspects that should be considered by the definition of mobile system architecture are:

— biometric capture sub-process, carried out by face, fingerprint or iris capture unit;

— biometric verification sub-process, carried out by face, fingerprint or iris verification unit;

— document reading sub-process (if present), covering MRTD as well as Member States national ID cards;

— visualization of process and results, both for operator and the subject of biometric authentication process;

— integrity of mobile system (Root of Trust)[6][7];

— denial of service (hand-held device is supposed to be used only by authorized operator), what can be done e.g. with biometric verification of operator;

— connection to other systems (VIS, SIS, AFIS, etc.) with the focus on protocols and the integrity of such connection.

Only first two aspects are in the scope of this document, and also the denial of service if performed through biometric verification. The other aspects are covered with the documents in Bibliography and not in detail considered in this technical specification.

In general there are two recommended options for the implementation of a biometric verification process for mobile system (score and quality driven methods) and they are in detail described in CEN/TS 16634 [3].

5.4.2 Physical and logical structure

There are two general physical structures of mobile system architecture.

— Physical bodies that contain the processing unit/elements, display, input and control, communication as well as all the sensors (all-in-one mobile solution), Figure 1.

— Physical bodies that contain sensors but need a separate device as processing / communication unit (“dedicated” peripheral) Figure 2.

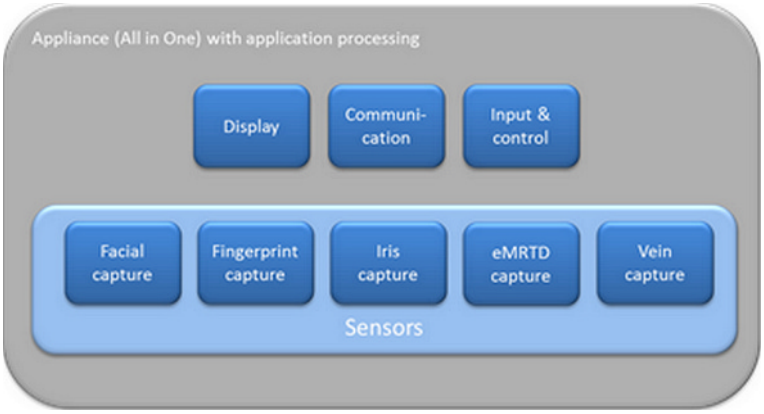

Figure 1 — All-in-one mobile system, containing different elements and biometric sensors

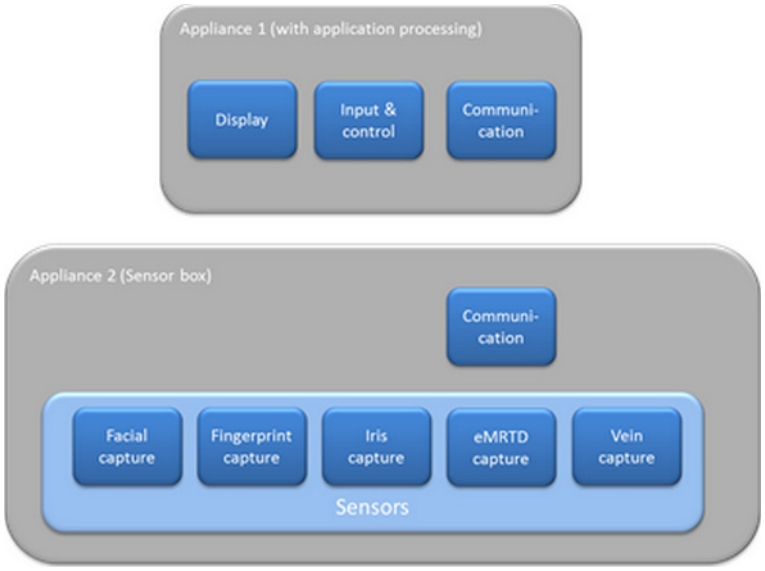

Figure 2 — Distributed system, two-device approach: one display and command unit, and the second one for capturing of biometric data)

The architecture for both approaches can be seen in Figure 3 (all-in-one) and Figure 4 (distributed system).

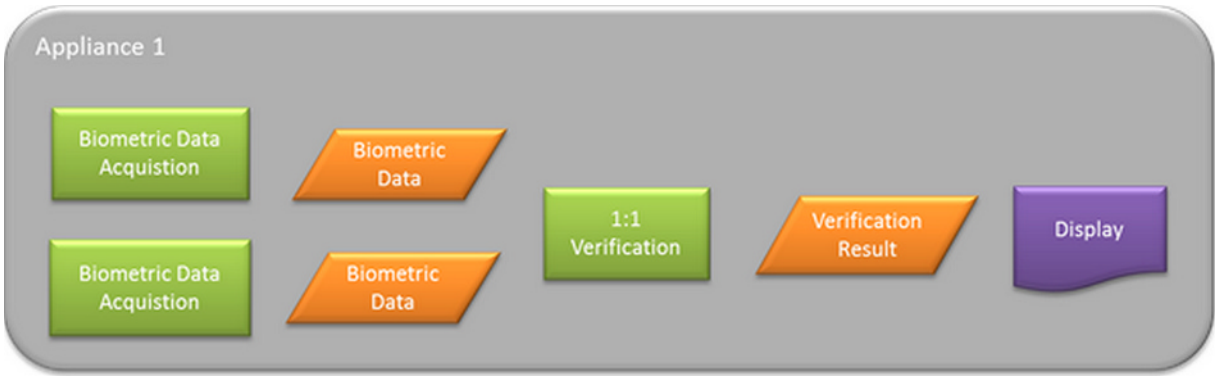

Figure 3 — 1:1 verification in one appliance, biometric data and result do not leave appliance

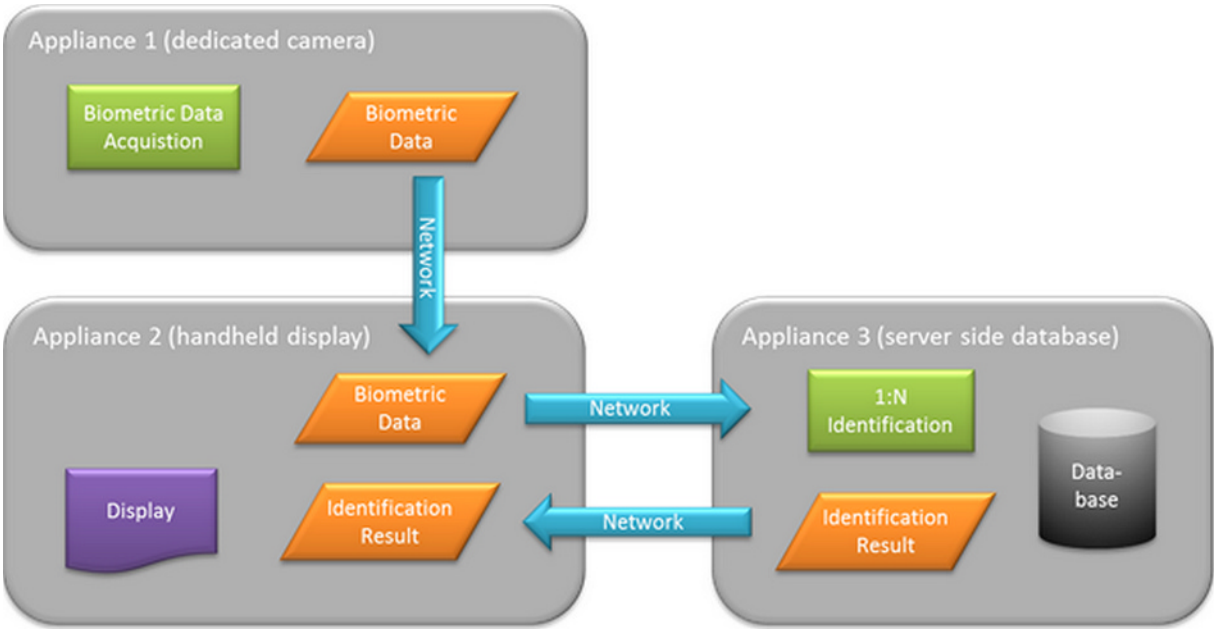

Figure 4 — An example of distributed system for 1:N identification in remote database

5.5 Biometric security functions

Member States can define specific process flows in order to ensure compliance with EU and national border control regulations.

Since environment is not well controlled, it is recommended that more than one biometric subsystem will be implemented. In case than one biometric system does not work due to environmental conditions (for example, illumination conditions for face verification) other systems should check biometric data. Biometric systems that can work in degraded conditions could send a notification (for example face or image quality) to operator or to a final data fusion or multibiometric subsystem. If the final part of the system is a data fusion subsystem or multibiometric system, scores obtained from degraded systems could be penalized.

It is recommended to use interfaces according to BioAPI for the capturing of biometric data. However, the operator of portable system may also allow proprietary vendor specific SDK interfaces for the integration of the capture unit.

For the portable biometric authentication system could be assumed that an operator will be near the system so it could be easily checked that only one person is using the system at the time.

5.6 Biometric sensors

5.6.1 General

The choice of the most appropriate biometric sensor has to be done considering a number of different constraints and requirements. The choice is important for any biometric identification system but for a mobile system the choice is even more important and critical. Choosing a sensor with specifications higher than the real needs may increase the mobile system's size, weight and cost, while a sensor with specifications lower than the real needs can impact the mobile system's accuracy and performance.

The choice of the biometric sensor has to be done considering the applicable use cases, such as:

— biometric enrolment;

— biometric verification;

— biometric identification.

In the enrolment phase, the biometric reference sample is captured, in order to be stored in a database or in a travel document. All the following verification and identification activities will be done by comparing a new sample with the reference sample captured during the enrolment phase and it is important to have a reference sample of the highest quality and containing as much details as possible. This is a pre-requisite to achieve high level of accuracy and performance of the biometric system.

Even though it is technically possible to perform biometric enrolment with a mobile system, in the context of this document we are not considering this usage scenario.

Biometric Verification is the use case that has the lowest requirements for the sensor, especially if the reference sample has been captured with a high quality sensor. For this use case, lower cost sensors can be used, allowing to design and manufacture smaller, lighter and more economical mobile systems.

In the biometric identification use case, it may be required to search a new biometric sample in a database potentially containing several millions biometric records. Thus a higher quality sensor is needed.

In the US, the NIST "Mobile ID Device Best Practice Recommendation" [9] also considers, in the choice of the biometric sensors, the applicable "risk level" of the usage scenario. For example, a "severe risk" scenario implies the possibility of loss of life and/or property if the biometric verification or identification is incorrect. The sensors recommended in the following chapters assume a "moderate" risk level: in a usage scenario with a higher risk level, it is recommended to use biometric sensors with higher specifications.

Sensors used in operational environments should be certified by an accredited certification body compliant with EN ISO/IEC 17025 (or equivalent).

In the following chapters more detailed guidance will be provided on fingerprint sensors and face image sensors.

5.6.2 Fingerprint sensors

A fingerprint sensor can either be a peripheral (wired or wireless) device or integrated into a mobile ID device. A Mobile ID device can be implemented either as a self contained unit (a single box) with the communications embedded in the device, as a peripheral or as a set of interconnected peripherals, each with its own function.

For fingerprint based biometric verification (1:1), it is recommended to use sensors compliant to ISO/IEC 19794-4:2011, B.2.

For fingerprint based biometric identification (1:N), it is recommended to use sensors compliant to ISO/IEC 19794-4:2011, B.3 and to capture at least two fingerprints.

The fingerprint sensor should provide fingerprint images of good quality within the full range of environmental conditions that could be encountered by the mobile device (e.g. bright sunlight, indoors, humidity, temperature). If a specific condition affects the performance of the biometric system, it is important to have given this information to the operator during the training for the use of the mobile device. For instance, if a fingerprint sensor may not be appropriate for use in direct sunlight, in this case, the operator should try to place the mobile device under a cover protecting it from direct sunlight. Detailed description of an environmental testing methodology can be obtained in [10].

NOTE To reduce the time that it takes to verify the identity of the document holder capturing several fingerprints at the same time can be considered.

5.6.3 Face image sensors

The parameters of the camera should ensure the provision of face images within a broad range of environmental conditions (e.g. bright sunlight, overcast light, indoors, additional lighting at night, differing distances and positions from device to subject).

It is recommended to perform a quality assessment on the captured images for providing good quality images to the verification process. The quality assessment should cover at least face and eye finding. ISO/IEC 19794-5 gives guidelines for image quality analysis. Additionally, quality assessment might be useful for test and evaluation purposes. It is recommended to provide uncompressed or lossless compressed live images. In any other case it should be ensured that the loss of information has no significant impact on the recognition performance of the face verification unit. Detailed description of an environmental testing methodology can be obtained in [10].

NOTE Light sources that illuminate at least the face area can be used to produce images of acceptable quality in dark situations.

5.6.4 Iris sensors

An iris sensor should be able to capture the biometric data ensuring good performance under the variety of environmental conditions of use for the mobile system (e.g. bright sunlight, indoors, humidity, temperature). The images captured by the iris sensor should have good quality considering all these parameters: eyes wide open, iris centred and fully visible, eyes looking at the sensor, sharpness, few reflections or specular highlights, left / right eye distinction. It is recommended to use a sensor compliant to ISO/IEC 19794-6:2011, Annex B. Detailed description of an environmental testing methodology can be obtained in [10].

5.7 Biometric algorithms

The maximum time necessary for the biometric verification (and, additionally, the maximum number of attempts) should be set in a way to avoid acceptance issues. The system should give feedback about the current status shortly after the process has started. The maximum time and number of attempts set depend on the application case and should be established taking into consideration accuracy and throughput constraints.

System vendors should state the expected FAR and FRR, and this statement should be verified by analysing operational data, e.g. by doing offline verification replay. It is recommended that the achievable performance of the biometric verification algorithm is measured by an independent test laboratory at regular intervals.

For live operation of the system, it is recommended to determine a proper algorithm configuration based on image data and verification results from the actual operational environment and a representative catalogue of test users and not to rely only on the standard configuration of the algorithm provider. It is recommended to monitor the error rates (especially the FAR) continuously or at least periodically (e.g. once a year) and to adjust the configuration if needed. . It is recommended to include a subsystem for the logging of statistical and technical data regarding the biometric verification and identification process, for the purpose of having a continuous quality control, extraction of business statistics and improvements of the systems.

Algorithms used in this kind of systems should be evaluated using test procedures to replicate operational conditions guided by ISO/IEC 19795 (or equivalent). Especially FAR/FRR/thresholds and other parameters involved in results of verification/identification process should be defined according to operational conditions in law enforcement scenarios.

For instance, generally is accepted that in access control to buildings environments a ratio FAR/FRR that help to quick access is expected. In law enforcement environments, usually, is more important to

minimize FAR. So, same algorithm may offer different results depending of operational conditions due to different expected results.

To satisfy the performance requirements of the application for any variation in the operational environmental conditions, parameters or calibration should be adapted automatically or be tunable by authorized staff.

5.8 Network performance

The throughput performance might be affected by communication rate. Recognition rate in portable systems will be influenced by the biometric solution and the data to be transmitted. Depending on available communication facilities, different kind of biometric data can be sent or received e.g. for fingerprints minutia or full image of the finger.

6 Application profiles

6.1 Introduction

At least two situations can be identified in which portable identity verification systems can be applied. In the first one, the system is placed in a fixed location (for example a road). Portable border control device is not fixed to this point (can change) but once installed, placement is fixed. Biometric control is done in that location. This use case can be covered by stand or workstation systems. Second one is a use case where the hand-held portable identity verification system is moved to the subject. For example in a bus or a train, a hand-held device can be moved while passenger stays in its place.

6.2 Transportable systems

6.2.1 Profile description

In this situation, the portable identity verification system is placed in a fixed situation (for example a road). Portable identity verification systems are not fixed to this point (can change) but once installed, placement is fixed. This type of systems could be unpacked and start operating without civil engineering works and in short time. Biometric identification is done in this situation.

NOTE The authority needs to ensure that the system is compatible with all eMRTD according to ICAO Document 9303 and all other eligible identification documents specified by EU or Member State legislation in scope of the desired usage scenario.

6.2.2 Environment description

Equipment size and weight could be similar to that in a fixed ABC. Since once the system was placed will stay for a period of time, special attention should be placed to find the best environmental conditions for biometric comparison. More than one system can be supervised by one border guard.

6.2.3 Biometric security description evaluation

The subject puts his/her passport or other document open by the data page (or trusted token) on the document reader. The system reads the biometric data contained in the document, or calls the stored reference data from a reference database (if a token without data storage capacity is used).

For eMRTDs security protocols should be used. In case of using a reference database appropriate security mechanisms should be implemented.

The biometric verification component should compare the user's biometric data captured live with those acquired as his/her reference data.

The maximum time necessary for the biometric verification (and, additionally, the maximum number of attempts) should be set for the system in a way to minimize the burden for the capture subjects. The

system should give feedback about the current status shortly after the process has started. The maximum time and number of attempts set depend on the application case and should be established taking into consideration accuracy and throughput constraints. Typical response time is:

— 5 s for local verification;

— 3 min for central AFIS identifications.

System vendors should state the expected error rates according to ISO/IEC 19795 and stating the conditions under which they have been obtained. This statement may be verified by analysing operational data.

It is recommended that the achievable performance of the biometric verification algorithm is measured by an independent test laboratory at regular intervals.

6.3 Hand-held systems

6.3.1 Profile description

This profile is applied to a system that has to check a bus, a train or a car queue or to a system used for identity verification in the field.

Access to fingerprint and/or iris in the RFID chip is protected by the EAC protocol, and the hand-held system shall use digital certificates to retrieve the biometric data. The central backend system delivers the certificates to the hand-held device using secure connectivity. In standalone mode, the certificates shall be preloaded in a Secure Access Module (local safe) of the hand-held device.

Hand-held system for identification can operate without database connection, by comparing the biometric data stored in the RFID chip of the document and the live biometric data of the holder. Remote or local database connection is not mandatory.

Portable identity verification system is held by the operator and passes across a queue of subjects (subject can be stand-on or seated). In some cases portable identity verification systems could be shared between the subject and the operator (for example to acquire fingerprint). In this case, operator will acquire subject image and give fingerprint sensor to the subject. Since interaction between system and subject could be maintained to a minimum, system could inform operator about the messages to read to subject. Care shall be taken to ensure that the subject is unable to read potentially confidential information displayed on the portable system screen.

Information about image quality should be given to operator to guide acquisition procedure.

6.3.2 Environment description

Portable devices are usually not operated in controlled environments, which might decrease the performances of the portable identity verification system. For instance the lighting conditions can affect the accuracy performances for face applications.

In these systems, equipment is moving from one subject to another. Environmental conditions can change from one subject to another, so conditions are completely uncontrolled.

The hand-held device should allow the capture of biometric data in the anticipated environmental conditions according to the operational scenario.

Sensors of mobile devices are potentially more exposed to dust and humidity and therefore they should be more robust and tolerant against these conditions.

Hand-held devices that utilize contactless technology will provide hygienic advantages.

The hand-held device should be able to be used in both outdoor and indoor environments.

The hand-held device should be fully functional across the operating temperature conditions, this includes the biometric functionality. Other characteristics as drop resistance are relevant but should follow the rules for law enforcement devices.

6.4 Workstation systems

In addition to transportable systems and hand-held systems, there is a third category that could be added: portable workstations (consisting of a desktop identity verification system in a portable enclosure such as a suitcase or a kiosk). A portable workstation can be equipped with sensors such as full page passport reader (allowing verification of physical security features) and larger fingerprint scanner. This kind of system could be used for example in airports where Schengen border controls are temporarily activated or in sea ports to verify passengers of cruise ships or cargo ships.

This profile is applied to a system that has to check a queue of users at the deployed location. The system will require infrastructure ie desks, illumination and access to electrical power supply.

Bibliography

[1] Guidelines on electronic — Machine Readable Travel Documents & Passenger Facilitation. Version — 1.0. April 17, 2008. http://www.icao.int/icao/en/atb/meetings/2008/TAGMRTD18/TagMrtd18_wp03.pdf

[2] Grant Agreement BC/CEN/ENTR/000/2007-23 — Final Version of the conformance/interoperability report – 2009-06-11

[3] CEN/TS 16634:2014, *Personal identification - Recommendations for using biometrics in European Automated Border Control*

[4] FRONTEX, Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems. Version 1.1. Warsaw, March 2011.

[5] ISO/IEC/TR 24714-1, *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance*

[6] Roots of Trust in Mobile Devices, ISPAB, February 2012, Andrew Regenscheid, NIST — national Institute of Standards and Technology

[7] Securing the core root of trust (malware, counterfeiting and IP theft in hardware), Ramesh Karri, ECE Department, NYU — New York University

[8] ISO/IEC 29197, *Information technology — Evaluation methodology for environmental influence in biometric system performance*

[9] NIST. “Mobile ID Device Best Practice Recommendation”. http://www.nist.gov/itl/iad/ig/upload/MobileID-BPRS-20090825-V100.pdf

[10] FprCEN/TS 16920:2015, *Environmental influence testing methodology for operational deployments of European ABC systems*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.