TECHNICAL SPECIFICATION

ISO/IEC TS 22604

First edition
2023-05

Information technology — Biometric recognition of subjects in motion in access-related systems

Technologies de l'information — Reconnaissance biométrique de sujets en mouvement dans les systèmes d'accès

Reference number
ISO/IEC TS 22604:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives) or www.iec.ch/members_experts/refdocs).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents or the IEC list of patent declarations received (see patents.iec.ch). ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The purpose of this document is to provide guidance on the use of in-motion biometric recognition technologies in access-related systems, where the previous enrolment and management of the identity of individuals needing access is required.

To satisfy increasing security demands, biometric recognition technologies are used in access-related systems to provide a more robust approach to identity authentication, and to mitigate security risks. However, this can come at a cost of increased processing times and lead to delays in user identification or verification.

Biometric identification and verification should be comprehensive and flexible for effective use in an access-related environment. Solutions should reduce user burden, be easy to manage, cost effective, maintain the security requirements, and provide permission-based access and global interoperability as necessary. Biometric systems should effectively allow authorized users' access, incorporate mechanical and behavioural mechanisms to refer unenrolled persons to human personnel and alert facilities to unauthorized users attempting to gain access. Systems should also provide a seamless, accurate and non-invasive user experience.

Considerable improvements in the performance of in-motion biometric recognition, have resulted in applications that enable automated, convenient and non-intrusive face, iris or fingerprint recognition across a range of scenarios including border control, passenger flow facilitation, access control and work place time and attendance. This provides a positive and non-intrusive user experience, as the user does not need to carry anything or stop and stand still to be recognized and does not need to touch anything.

There are several considerations that are unique to in-motion biometric solutions for design of contactless biometric recognition systems. Design considerations include:

- Selection and placement of biometric data capturing devices (e.g. cameras).
- Control of the flow of individuals requiring access to ensure that only those that are authorized gain access.
- Proximity of capture devices to individuals seeking access for the contactless in-motion capture of the needed information. The proximity of the biometric capture devices can depend on the employed biometric modalities.
- Management of exceptions.
- Mutual placement of capture devices and equipment dedicated to physical access-control (e.g. door, barrier, turnstile).

A number of use cases involving in-motion biometrics address different scenarios including:

- where access is on the basis of the prior enrolment of all individuals well in advance of interacting with the biometric system (identification);
- where access is on the basis of credentials presented just prior to interacting with the biometric system (verification) (e.g. wireless technology, RFID token or a vehicle number plate or any other token available without any interruption to the person's flow of movement).

These scenarios present different challenges to in-motion verification and identification processes.

Critical to the success of biometrics-based secure access is implementation of state-of-the-art data protection technology and procedures (see ISO/IEC 20889[1] on privacy enhancing data de-identification techniques, according to the privacy principles established in ISO/IEC 29100,[3] taking into account legal, common practice, business, industry and privacy considerations).

An important factor in in-motion biometric recognition is its ability to sense/detect presentation attacks per ISO/IEC 30107-3.[5]

Information technology — Biometric recognition of subjects in motion in access-related systems

1 Scope

This document establishes requirements for development of biometric solutions for verification and identification processes for secure access without physical contact with any device at any time. The solution acquires the biometric characteristics that are captured while the data subjects are in motion to verify or identify the individuals requiring access, and thus controlling access using contactless biometrics.

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 19795-1, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 19795-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
in-motion identification
identification for which a person in motion can be identified without physical contact with any device at any time

3.2
non in-motion identification
identification for which a person needs to stop to be identified

3.3
in-motion verification
verification for which a person in motion can be verified without physical contact with any device at any time

3.4
recognition area
area where biometric characteristics are captured and biometric recognition can be performed

3.5
attraction point
distraction in the field of view of the people in the recognition area that pulls the attention of the people making them look in a specific direction

3.6
access point
location, typically with a physical barrier, where users are identified and pass through to enter an access-controlled area

3.7
feedback signal
signal for the identified user providing him or her information on the status of his or her access authorization

3.8
authorized user list
list containing the information and biometrics for identifying authorized users

3.9
unauthorized user list
list containing the information and biometrics for identifying unauthorized users

3.10
alert list
list containing the information and biometrics for identifying unauthorized users for which an alert needs to be raised in case of identification

4 Biometric recognition in motion

4.1 General

4.1.1 Purpose and constraints of in-motion biometric system

In-motion access-related systems allow users to be identified without stopping and without any physical contact with any device. The targeted optimal solution should be handled to grant access to an area using biometrics without asking the users to perform any specific action and without any additional constraint on them compared to a crossing without biometric identification. However, the live biometric data needed to identify the users should be as good as possible to avoid a false rejection, and this tends to add constraints on the users (e.g. look in a specific direction, perform a specific action like removing their glasses). At the end, it is all about the user experience; additional constraints on how to behave while crossing the access control point are bad for the user experience. One of these constraints is to be obliged to stop, and in-motion systems try to remove it. But a false rejection of an authorized user is also a very bad experience for them and should be avoided in any case. Therefore, there is a trade-off to find between a complete freedom of movement and behaviour and the constraints added to the user to get captured with good quality images. One positive aspect is that, in the authorized user list use case, the biometric capture subject wants to get access to the secured area protected by the biometric check and can be expected to be more or less cooperative. In this case, there is definitely a way to provide a good user experience with an in-motion system with low FTA and low FRR.

A biometric system can be considered in-motion when subjects do not stop/pause for the biometric capture process. They can slow down and perform few actions (without any physical contact with a sensor). It is not required that all authorized users cross the access control point without stopping but most of them should be able to. The operator should decide the trade-off between convenience and security depending on the application.

Systems for secure and effective recognition of individual people are essential for the management of many types of facilities, including office buildings, residential facilities, private clubs, campuses and other locations that include sensitive and/or private assets. They are also needed to secure borders.

There are three cases used to recognize users for access-related applications:

- biometric verification of a provided credential;

- biometric identification against a database of pre-enrolled people;
- multi-factor authentication using biometrics for identification and for verification and a token as a secondary means of authentication.

From the viewpoint of user actions, there are:

- non in-motion identification or verification – the user is required to stop in the recognition area to be properly identified or verified;
- in-motion identification or verification - as the user is approaching an access point from a distance, he or she is identified or verified without any stop or physical contact with any device.

4.1.2 Biometric performance and error rate

The challenge for in-motion access-related systems is to limit the increase of false rejection due to the lower quality of the images captured in motion compared to non in-motion systems. This can be achieved by different means like using more robust detection and matching algorithms, dedicating the hardware to in-motion capture, ensuring the quality of the enrolment data, putting constraints on the environment, improving the user interface and overall ergonomics or even limiting the database size.

Like for all biometric systems, biometric accuracy of in-motion system needs to be expressed in terms of failure to acquire rate (FTAR), a false acceptance metric (FMR for verification system, FPIR for identification) and a false rejection metric (FNMR in verification, FNIR in identification). The specificities of in-motion biometric systems actually concern the FTAR and the FNMR/FNIR, but should have no impact on the security level, meaning the FMR/FPIR.

The technical levers include:

- more robust detection (improve FTAR) and biometric comparison algorithms (improve FNMR/FNIR);
- dedicating the hardware to in-motion capture (improve on FTAR and FNMR/FNIR, see 4.1.3);

  EXAMPLE The system uses camera with smaller shutter speed or higher frame per second rate. The camera is motorized to focus on a refined region of interest.

- ensuring the quality of the enrolment data (improve on FNMR/FNIR, see 4.5);
- putting constraints on the environment as lighting (improve on FTAR and FNMR/FNIR);

  EXAMPLE With a shutter speed optimized for in-motion capture, a too dark acquisition environment results in weak signal.

- optimizing the database size (improve FNIR);

  EXAMPLE Dataset is carefully maintained in order to only have the relevant and current users registered for a specific access control point.

- improving the user interface and overall ergonomics (improve FTAR, see Clause 5);
- improving mutual placement of capture device and equipment dedicated to physical access control (e.g. door, barrier, turnstile) (improve FTAR, see 4.6.1).

4.1.3 Quality/speed compromise

For many biometric modalities, the quality of a sample captured in motion is lower than that of a sample captured without motion. This assumption is valid for several reasons:

- For photographic reasons, images taken in motion can be darker, less contrasted, with lower resolution, and noisier than the static images. For instance, for in-motion biometric capture, it is interesting to have a large depth of field (get a focused image in a wide depth range in order to maximize the number of images that can be used for biometric feature extraction) and then decrease the aperture. In the same time, motion blur should be avoided, and a small shutter value should be used.

EXAMPLE 1 When the acquisition is performed in motion for face recognition modality, good practice to prevent motion blur is to use a shutter speed from 1/125 s to 1/50 s for a normal walking rate of around 1 m/s to 1,5 m/s. These two settings decrease the amount of light coming on the photographic sensor and then produce darker and less contrasted images. A way to get brighter images is to illuminate the scene more strongly but there are limitations on user acceptance and experience. Another way is to use higher ISO values, but this will bring electronic noise on the captured image. As the images can be captured from a longer distance than in static mode where the user is standing in front of the biometric capture device, resolution can also be smaller, decreasing the global quality of the biometric data.

EXAMPLE 2 For face recognition modality, good practice regarding resolution is 10 pixels per centimetre on the face.

- Time to acquire a valid image is much smaller in motion than statically. When the user stops and looks at the device, or places their finger on a sensor, there is time to choose images of sufficient quality while the user doesn't move. In opposite, in the in-motion biometric capture, the user is moving during the acquisition and the biometric decision should be taken at the latest when the biometric capture subject reaches the access point.
- Considering that the system should be as seamless as possible, the available images that are valid for a biometric comparison are much fewer because the user has very limited interaction with the biometric capture device. Even in a cooperative case, the main purpose of an in-motion system is to have as low impact as possible on the user normal behaviour, thus leading to few exploitable images.

The challenge for in-motion access-related systems is then to limit the increase of false rejection rate, due to the lower quality of the images captured in motion:

- more robust algorithm able to deal with various acquisition environments and behaviours from data capture subject;
- capture device hardware improvement;
- constraints on the capturing environment;
- ergonomics/user interface;
- limitation of the database size.

4.2 Biometric verification vs. biometric identification

4.2.1 Implementing an in-motion verification system

When implementing biometric verification, the way to provide the biometric reference shall be specified. The individual can provide directly the reference biometric data to the system (for instance, presenting a smartcard or other token where the biometric reference is stored or scanning a 2D barcode containing a biometric template), or use credentials allowing the access to the reference biometric data stored in a database (using a contactless card or a PIN code). These examples show interactions of the user with a reading device, which is not compatible with a fully contactless and in-motion access control system. However other solutions can be implemented to keep a seamless use of an in-motion access control system in verification mode.

The idea is to design an access control system which is able to retrieve biometric reference data from the user without any action from the user approaching the system. Such a system should be able to sense the user when he/she is in a predefined area around, and to retrieve the necessary reference data for future use. This can be achieved by a wireless connection between the system and a token possessed by the user, which can be any connected device.

EXAMPLE The token is a smartphone.

When the user approaches the system, the token is detected and starts communicating with the system, exchanging the necessary data even before the live user biometrics is captured. When closer to the access control point, the live user biometrics is captured, and compared against the reference data (biometric verification). If access is granted, the user can go through without stopping and touching anything.

If multiple tokens can be present and detected at the same time with ambiguity about which one belongs to the individual trying to gain access, some mechanisms need to be implemented.

The live biometrics should be matched against the closest one, but can also be matched against the reference data of all detected present users, giving access if one of them is considered as genuine. The sensing area should be small enough to avoid that too many users are considered as possible candidates, but needs to be large enough to detect users as early as possible to allow in-motion, no stop access.

4.2.2 Implementing an in-motion identification system

When the biometric capture subject approaches the access point, biometric probes are captured and searched against the reference database (biometric identification). The identification system should be configured such that the candidate list includes only candidates whose similarity score exceeds an acceptance threshold. If access is granted, the user can go through the access point without stopping and touching anything.

4.3 Process flow in access-related systems

Possible process flows include:

- All users are authorized if the biometric data quality is good and the user was not identified in the unauthorized user list.
- Only users in the authorized user list are accepted.
- Both authorized and unauthorized user lists exist in the system. Operators should decide what to do when a user is identified in both lists.
- Users on an alert list signal an alert. Additionally, system operator can treat alert list as authorized user list or as unauthorized user list.

For unattended systems, it should be defined by system policy whether alerts should be raised to an operator, just logged in a system log or both.

4.4 Applicable biometric modalities

4.4.1 General

In-motion biometric recognition can be based on any information obtained in a contactless/touchless way and supporting natural human behaviour. Different biometric modalities can be used, such as for example face, periocular region, hand/finger, iris, gait/anthropometrics, voice or a combination of modalities.

4.4.2 Face modality

The use of the face for in-motion biometric recognition is natural and contactless, with no physical interaction with the sensors, as a simple glance in the general direction of the capture device is generally enough.

This is the most common biometric modality for such a system. Facial image capture is non-intrusive, quite easy to achieve, and user acceptance is high.

4.4.3 Iris modality

Similar to face recognition, iris recognition can be done with only a glance at a camera. The main advantage of this biometric modality is its very high recognition accuracy, the main difficulty being to acquire good quality iris images.

This biometric modality was historically limited to intrusive acquisition devices, where the user needed to approach his or her eye very close or even touch the device. Latest improvements in iris acquisition devices allow now to capture irises at a distance and even in motion.

4.4.4 Fingerprint modality

The use of fingerprints for in-motion biometric recognition can be done by swiping or presenting the fingers in front of a contactless fingerprint sensor. Given an optimal position of the biometric capture device and good ergonomics, along with a fast image capture, this hand swipe would be possible while the user is still moving towards the access point.

4.4.5 Palm modality

The use of hand palm for in-motion biometric recognition can be done by swiping or presenting the palm in front of a contactless palm sensor. Given an optimal position of the biometric capture device and good ergonomics, along with a fast image capture, this hand swipe would be possible while the user is still moving towards the access point.

NOTE Capture of Ulnar characteristics (writer's palm, or side of hand) is not possible using biometric-recognition in motion technology (at the time of publication). Thenar (ball of hand/palm) capture is possible at the time of publication.

4.4.6 Complementary modalities

Some biometric modalities, like periocular or gait and anthropometrics, can be used in multimodal schemes to improve recognition accuracy.

For gait, the system should be designed in such a way that video of sufficient duration is captured for the intended biometric processing.

4.5 Enrolment and its quality

As stated above, the quality of the in-motion biometric data can be poorer than the one expected in standard non in-motion biometric systems. To ensure the global performance of the system, high quality biometric data is needed at enrolment. There is indeed a strong effect of the quality on the biometric performance of the system (false acceptance rate and false rejection rate). Consider a biometric algorithm able to compare two biometric data (whatever the biometrics used). This algorithm will achieve the best accuracy with the highest image quality on both sides (e.g. high resolution, no blur). When the quality is decreased on one side of the comparison, it will be more difficult to recognize this image and the false rejection rate will increase. However, the false acceptance rate should not be changed as this quality drop is not making the image looking more like the other high-quality image. But when both images have a poor quality (both are blurred for instance) they can look more like each other, and false acceptance rate will be increased as well.

As images captured in motion can be of lower quality (as stated above), and considering the effect of quality on biometric performance explained above, keeping high quality for the enrolment images is absolutely necessary. Applicable standards are ISO/IEC 19794[9] and the ISO/IEC 39794 series,[10] as well as ICAO TR on portrait quality[11] (for face biometrics).

4.6 Ergonomics

4.6.1 Capture device physical placement

The location of the sensor needs to enable natural behaviour of a person without the need to stop in order to be identified. This means that the capture device should be designed to fit with all user profiles, especially the height. It should not be invasive or too massive to not disturb the normal walk of the user. Typically, the device will be placed on one side of the walking area, and oriented to it, so that the user can simply have a look or take a simple action toward it while walking. Face or iris capture devices can also be placed on top of the walking area, even if this brings more constraints on installation.

Another very important point is the relative position of the biometric capture device and the crossing point of the access system (typically a door). In order to achieve a walkthrough process without stopping the user, the biometric capture, comparison and decision, and even the door opening should be finished when the person arrive at the door level at walking speed. If the capture device or the door opening is slow, this means that the capture device and the door should be widely separated from each other.

Tampering from attackers can be partially prevented by presence of human supervision. If no human is present, the system shall include tampering preserving mechanisms like all access control systems.

4.6.2 Catch attention

Subjects shall adequately cooperate with biometric sensors when in motion. This is especially the case for biometrics on-the-move applications where, for example, the subject is walking towards the sensor. If the subject is distracted then, for example, face, recognition cannot reach acceptable performance or fail completely. Attraction points (e.g. visual displays) may be used to pull the attention of the subject towards the sensor.

4.6.3 Feedback signal

As the recognition is performed in motion, feedback on the success or refusal of the recognition, would be provided to the user. The location of an audiovisual or just a visual feedback would be next to the sensor.

Upon successful recognition, the user may continue with the intended activity (ex. passing through the access point).

Upon unsuccessful recognition, the user would divert from the intended activity. It is advised that the feedback would instruct the user on a possible alternative action (e.g. try static recognition or ring the bell).

4.7 Biometric information storage

The way in which biometric information is stored can vary based on the use case and implementation details:

- biometric information stored in a persistent biometric database;
  - identification can be performed as a 1:N identification where the live information is compared to a database of all authorized users,
  - identification can be performed as biometric 1:N and verified using a token,

  - identity verification can be performed as 1:1 matching using biometrics linked with a token and a unique biometric identified stored in the database;
- biometric information stored in a temporary biometric database (e.g. passenger flow facilitation);
  - in some use cases, the user will be enrolled on-the-fly to a temporary database and will be identified at additional access points based on the temporary database;
- biometric information stored on a token;
  - in this process, the biometric process verifies that the holder of the token is the correct holder, comparing the live biometric information to the information on the token.

When a database is used, this database may be stored locally in the device or be a centralized database stored in a server where the biometric comparison will take place.

Using a database stored locally can optimize process time. If the database is stored in a server, data transmission time of the probe sample needs to be taken into account to guarantee fast enough process time. This is particularly relevant when multiple access points can try to connect simultaneously to the centralized dataset.

5 Accessibility, usability and guidance

5.1 General

Like all biometric systems, in-motion systems should follow the general guidance on accessibility and usability of biometric systems contained ISO/IEC TR 24714-1[2].

Compared to non in-motion system, in-motion systems should additionally consider issues specific to the intended usecase.

For example, while most non in-motion access control consist of a barrier which is opened after a successful verification, barriers should be opened by default to favour the flow of user's access.

In-motion systems also correspond to a usecase where the convenience of the user is prioritized. The users should be enabled to act as naturally as possible and no excessive burdens should be put on them. Quality checks and behavioural instructions which are required in more secure usecase should not be enforced for in-motion systems.

EXAMPLE An in-motion system does not require that the person has a neutral face expression or take off his/her glasses to claim access.

By design, an in-motion biometric system is intended to be resilient to a wide variety of presentation from the capture subjects, and should be adapted to most groups.

Like all biometrics systems, the system shall be as inclusive as possible and shall for example be evaluated in regard to potential performance differential related to demographic factors, using equity measures defined in Reference [8].

5.2 Accessibility

In-motion systems should follow the general guidance on accessibility contained in ISO/IEC 24714[2] and ISO/IEC TR 29194[4].

As convenience is the main focus, special care should be taken to take into account as many people as possible, but this can be even more difficult than for non in-motion systems. This needs to implement dedicated access point.

EXAMPLE 1 A building has six in-motion access points. Five are designed to deal with most of the population. The sixth one is specially designed to be more accessible. The gate is larger to facilitate access to wheelchair and the system has more tolerance and possibility to adjust the acquisition to various height. The access point also offers audio feedback additionally to visual cues to help people with sight issues.

Additionally, like for all biometric system, alternative process shall be offered for access.

EXAMPLE 2 Human supervisor is present to grant access in case of impossibility to be managed by the biometric system.

5.3 Usability

Signage shall clearly indicate that an in-motion biometric recognition access control system is in use. Users that are aware of a system in use can then cooperate with the system. Users should also be informed about any action they need to take, for example, looking at the capture device, or wave his or her hand on the fingerprint device, in order to reduce interaction problems.

The ISO/IEC 24779 series offers guidance on how to best convey visual information and instructions to users.

5.4 Acceptable delay for a user for fluid passage

The delay acceptable to a user to realize a frictionless implementation will depend upon the biometric sensor and deployment setting.

For example, for contactless fingerprint, the subject can slow down his or her walking pace and swipes their fingers in front of a contactless sensor.

As another example, if the system involves a physical barrier, while for non in-motion systems an acceptable transaction time can be several seconds before the feedback signal is provided and the subject is allowed to continue, for in-motion systems the processing time after the biometric acquisition should be shorter than the time needed to reach the barrier.

If no physical barrier is present, the processing delay shall be fast enough to allow a supervisor to stop the capture subject for further investigation just after the control point.

5.5 Guidance

In access-related biometric systems, a cooperative behaviour of users will enable high performance of the system and can therefore give the users the benefit of faster service. Cooperation means behaving in the right way to enable the biometric capture device to capture the biometric data (e.g. looking in the correct direction or placing/swiping a hand over the right sensor). In this way the biometric system can identify the user based on optimal quality biometric data, or reports whether the user is unidentified because the data quality was too low for a decision.

When using biometrics in motion, which is without contact or necessity for the user to stop, new or untrained users can only co-operate if they are aware of a biometric system. In case the user population can be unaware of the in-motion biometric recognition, or of the possibility to be unauthorized, the operator can place a sign with explanation.

Unauthorized user list systems should implement quality metrics in order to avoid fraudulent access of intentionally uncooperative unauthorized users. When quality is low, the user should be offered an alternate method to access. Low quality biometrics can be caused by fraudulent use, but can also be the result of other accessibility or usability issues. However, such needed actions from the user should be limited and even suppressed through an optimal design of the biometric capture device and possible additional signage. These needed actions from the user would indeed tend to make the process more complex and even end up to a stop of the user (which in-motion systems are intended to avoid).

NOTE For a list of relevant accessibility and usability issues, see ISO/IEC TR 24714-1[2].

6 Privacy and security considerations

6.1 Data protection

Biometric access-related systems can contain both non-biometric personal identifiable information (PII) and biometric information that can be used for identifying persons. Such information needs to be secured and protected against leaks and unauthorized access and/or use. There are several practical ways that such protection can be implemented, most of which involve encryption, use of irreversible biometric vectors and strong network security. It is critical that biometric systems provide protection for the PII of the user.

In implementations where data interchange is necessary at each transaction between the biometric sensor and a centralized reference dataset (as discussed in 4.7), network security will be of particular interest.

Cryptographic protocols similar or equivalent to state-of-the-art Transport Layer Security (TLS) protocol should be implemented. The PII data transfer between the sensor and the database shall be ciphered and there should be a mutual authentication between the sensor and the database.

6.2 Consent

In-motion biometric system are usually opt-in access-control system. As such, consent from the capture subject will generally be collected at enrolment stage. The consent is not collected again during verification and identification transactions as the intent is to have a system as fluid and fast as possible.

If people not registered in the system can access the control point, a clear marking should signify that a biometric acquisition will take place. This marking should be particularly explicit for modalities, like face, where only limited active interactions is required from the capture subject.

Also, for people not willing to take part in a biometric activity and not wishing to grand consent, alternate access means shall be offered not involving biometrics.

6.3 Presentation attack detection

In the majority of biometric access solutions, it is necessary to have effective Presentation Attack Detection (PAD) mechanism, such as described in ISO/IEC 30107-3[5], that identifies imposters trying to gain access by presenting an artefact replicating the biometric information of an authorized user.

PAD is more difficult in motion, or at least can involve different techniques than the one used in a non in-motion system.

For instance, for fingerprint, techniques exist that measure the electrical conductivity of the finger. As an in-motion system is seamless and contactless, such countermeasures cannot be used. In opposite, specific countermeasures which are not possible with contact can be used contactless.

Impact of lower quality of in-motion images also has an impact on the PAD rate.

Finally, multi biometrics and then PAD based on multiple biometrics are more efficient than one biometric modality only. It is harder to spoof both the face and the iris biometrics than the face only.

An access-control system should have mechanisms to reduce the risk of tailgating. These mechanisms often include multiple devices in order to be able to handle this task.

EXAMPLE Tailgating is detected by combining optical imaging and infra-red beams to detect and track people.

6.4 Security considerations

Biometric recognition of subjects in motion presents new challenges with respect to security. Potential vulnerabilities include unauthorized access to biometric templates, token replay, presentation attacks, network security (e.g. over a wireless technology) and unattended acquisition and trustworthiness with biometric sensors. There are several practical ways that such protection can be implemented, most of which involve encryption, use of biometric template protection schemes, PAD methods and strong network security.

7 Examples of deployment

7.1 General

In-motion biometric access systems can be deployed in different environments such as:

- airports and public places;
- public transportation;
- sports arenas and facilities;
- secured campuses and buildings;
- medical facilities.

7.2 Use cases

7.2.1 Example of system with fingerprint

A frictionless access control is deployed in a company's headquarters due to the sensitive nature of its activities in the building and to respond the traffic of employees. Most employees get to the office via nearby metro and tram stations, and therefore arrive within the same 30-min window. This creates the need for a high-throughput access control solution, for entrance and exit peak-times.

The company opted for a contact less sensor device associated to speed gates. Four gates were installed, with devices for entry and exit.

The device performs a 3D scan and verification of four fingerprints in less than 1 s, in a quick and touchless gesture within the reader. These features make the product particularly well-suited for such high-traffic locations, with the capability to authenticate up to 50 people per minute.

Instead of finding closed doors, users are instead welcomed with a fully open passageway and a distinctive system of visual identification. In the event access is not granted, the gate doors will close in proportion to the proximity and speed of the non-authorized user.

Employees appreciate the frictionless use of the device, as well as gate’s “always open” concept, that enables them to get to the elevators in only a few seconds. See Figure 1.

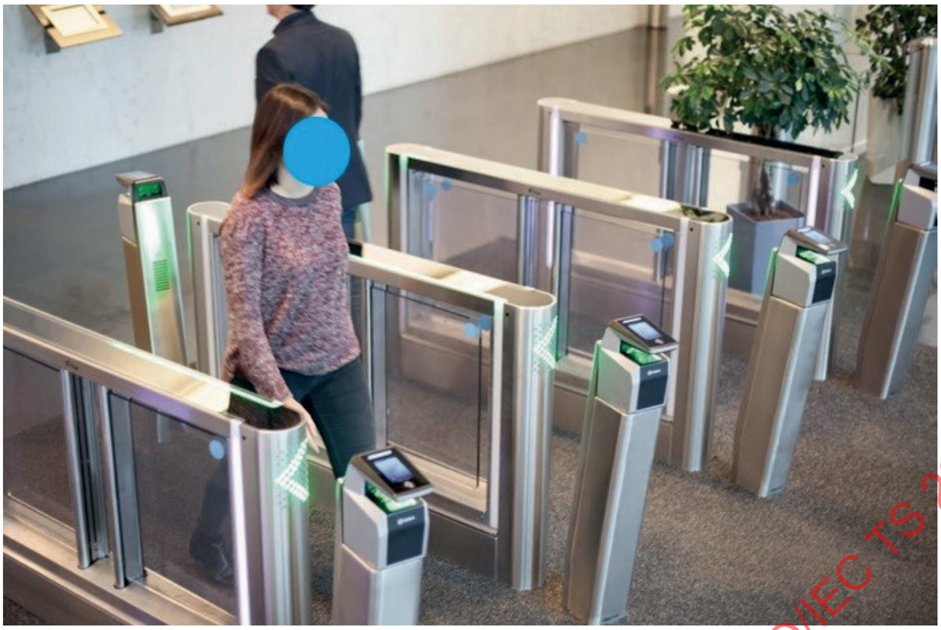

Figure 1 — People crossing in-motion biometrics gates

7.2.2 Example of system with multimodal biometrics

An EC funded project[12] explored how advances in biometric technology promises improved security solutions for borders while simultaneously improving the traveller's experience through expedited crossing of the border. Specifically, the project investigated and proposed new less obtrusive approaches to biometric data capture and verification, particularly the use of emerging and contactless multimodal biometrics including hand vein, periocular and anthropometrics modalities.

Moreover, the project explored how traveller identification can be performed on-the-move whereby the in-motion identification process takes place indoors (within a monitored access corridor where the traffic flow is controlled), or outdoors with travellers in vehicles in a non in-motion identification setting.

The identification process is in two stages. In the first stage – enrolment – travel document data and multiple biometrics are captured at a kiosk in a supervised manner via an informed consent process (see Figure 2). The collected data is encrypted and downloaded securely to the traveller's smartphone within the project app. If required, enrolment can minimally be performed once per lifetime of the travel document, and multiple biometrics enrolled in one step and used for verification both in the traveller-on-foot and traveller-in-vehicle use cases.

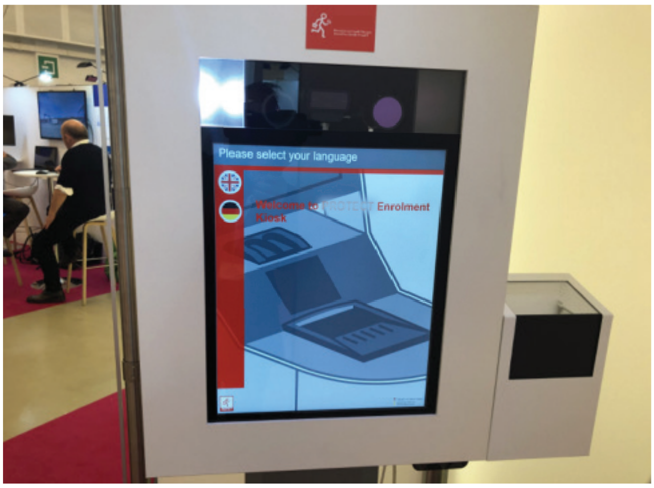

Figure 2 — Enrolment kiosk

In the second phase – recognition – the identification process begins when the traveller arrives at the border and approaches the recognition area. Once the traveller is in close vicinity of the recognition area, the project app on the traveller's smartphone processes signals sent by a nearby installed indoor positioning system to inform the system that the traveller is about to pass through the recognition area. Then, the project app transfers the set of encrypted travel document and biometric data to the border control system. The transferred data is temporarily stored only for traveller verification within the recognition area. See Figure 3.

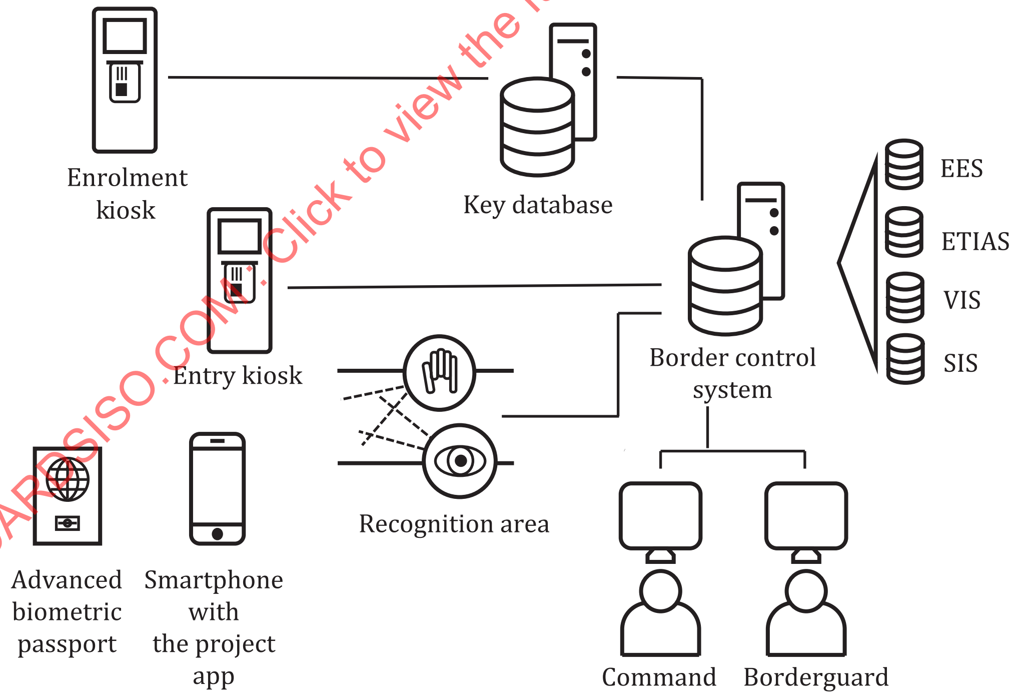

Figure 3 — Overall system architecture

As the traveller enters the recognition area at the border, live biometrics are captured, verified and fused (according to ISO/IEC TR 24722:2015[6]) in real-time. The process also incorporates presentation attack detection, according to ISO/IEC 30107-3[5], and detection of evasion of the identification process itself. Before the traveller reaches the end of the recognition area, a feedback signal is communicated simultaneously both to the border guard via a handheld device (or optionally a mixed-reality headset) and to the traveller via their smartphone project app. If a traveller is not identified, is deemed to be