Received: 10 December 2021 | Revised: 9 December 2022 | Accepted: 15 January 2023

IET Biometrics

DOI: 10.1049/bme2.12107

The Institution of Engineering and Technology WILEY

CASE STUDY

Facilitating free travel in the Schengen area—A position paper by the European Association for Biometrics

Christoph Busch[1] | Farzin Deravi[2] | Dinusha Frings[3] | Els Kindt[4] | Ralph Lessmann[5] | Alexander Nouak[6] | Jean Salomon[7] | Mateus Achcar[8] | Fernando Alonso-Fernandez[9] | Daniel Bachenheimer[10] | David Bethell[11] | Josef Bigun[9] | Matthew Brawley[12] | Guido Brockmann[13] | Enrique Cabello[14] | Patrizio Campisi[15] | Aleksandrs Cepilovs[16] | Miles Clee[17] | Mickey Cohen[18] | Christian Croll[19] | Andrzej Czyżewski[20] | Bernadette Dorizzi[21] | Martin Drahansky[22] | Pawel Drozdowski[23] | Catherine Fankhauser[24] | Julian Fierrez[25] | Marta Gomez-Barrero[26] | Georg Hasse[27] | Richard Guest[2] | Ekaterina Komleva[28] | Sebastien Marcel[29] | Gian Luca Marcialis[30] | Laurent Mercier[31] | Emilio Mordini[32] | Stefance Mouille[33] | Pavlina Navratilova[31] | Javier Ortega-Garcia[25] | Dijana Petrovska[34] | Norman Poh[35] | Istvan Racz[36] | Ramachandra Raghavendra[1] | Christian Rathgeb[23] | Christophe Remillet[37] | Uwe Seidel[38] | Luuk Spreeuwers[39] | Brage Strand[40] | Sirra Toivonen[41] | Andreas Uhl[42]

Correspondence
C. Busch.
Email: christoph.busch@ntnu.no

Abstract
Due to migration, terror-threats and the viral pandemic, various EU member states have re-established internal border control or even closed their borders. European Association for Biometrics (EAB), a non-profit organisation, solicited the views of its members on ways which biometric technologies and services may be used to help with re-establishing open borders within the Schengen area while at the same time mitigating any adverse effects. From the responses received, this position paper was composed to identify ideas to re-establish free travel between the member states in the Schengen area. The paper covers the contending needs for security, open borders and fundamental rights as well as legal constraints that any technological solution must consider. A range of specific technologies for direct biometric recognition alongside complementary measures are outlined. The interrelated issues of ethical and societal considerations are also highlighted. Provided a holistic approach is adopted, it may be possible to reach a more optimal trade-off with regards to open borders while maintaining a high-level of security and protection of fundamental rights. European Association for Biometrics and its members can play an important role in fostering a shared understanding of security and mobility challenges and their solutions.

KEYWORDS
biometrics (access control), biometric template protection, biometric applications, computer vision, data privacy, image analysis for biometrics, object tracking

1 | INTRODUCTION

The European Commission has recently established a Schengen Forum in order to discuss, in a gathering of the member state Ministers of Home Affairs and Members of the European Parliament, measures to reinforce common security and mobility in the Schengen area. This forum is needed in order to re-establish and guarantee the functioning and benefits of the Schengen area and maintaining its security. This requires common action at European Union level and constant efforts from all Member States [1]. In spite of the legal commitments established by the Schengen treaty, recent incidents in the last 6 years have created a reality of border controls between member states. New technologies and innovation shall be explored, to achieve the Schengen objective, by discussing best practices and identifying the role of security research and innovation. Recently the European Commission has issued a proposal for a regulation on a Union Code on the rules governing the movement of persons across borders [2] that intends to ensure the proper functioning of the Schengen area in order to put the ecosystem of rules back into balance and restore and reinforce mutual trust between Member States [2].

Generally speaking, such technologies can either be pro-active and prevent an incident (e.g. a terror attack) or re-active and help the criminal investigation of an incident, as it is illustrated in Figure 1.

The objective of this position paper is to identify possible technological solutions that can reinforce common security and free mobility in the Schengen area. Despite the promise of technology, we must acknowledge some of the corresponding limitations of the model presented in this paper: For internal borders, where required, there will be a need to achieve a compromise between seamless traveller flow, loss of privacy with the use of tracking technology and long transaction-times in border control. These may be considered as three vertices of a triangle. Decisions taken by European stakeholders and EU member states with regard to the use of novel technologies while addressing the regulations will lead to a specific operating point inside the triangle, as it is illustrated in Figure 2.

While prior to 2015 internal borders in the Schengen area were not controlled, in the year 2021 the reality is that internal borders are partially controlled or even closed for reasons discussed in the subsequent section. One of the consequences is that industry that relies on "just in time" delivery of supply goods, is facing disruptions of their production processes. The European society can now either lean towards the status with free movement and no interactive border control (and no waiting times) with selected deployment of new technology at borders for lawful identification of vehicles and/or individuals on 'watchlists' or return to a seamless travel without any internal border control and no recognition technology, which will constitute a full risk of being attacked as a society or maintain the status of 2021. Threats and risk for the society in the Schengen area are manifold and a full discussion of them is beyond the scope of this paper. However, the interested reader can find a good overview in the UK National Risk Register [3].

The issue of how to abolish the internal borders that some EU Member States have temporarily reintroduced on their territories after several terrorist attacks and the current

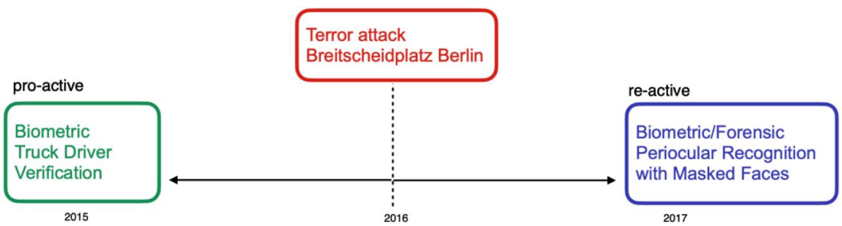

FIGURE 1 Pro-active measure, to prevent an incident and re-active measure in criminal investigations.

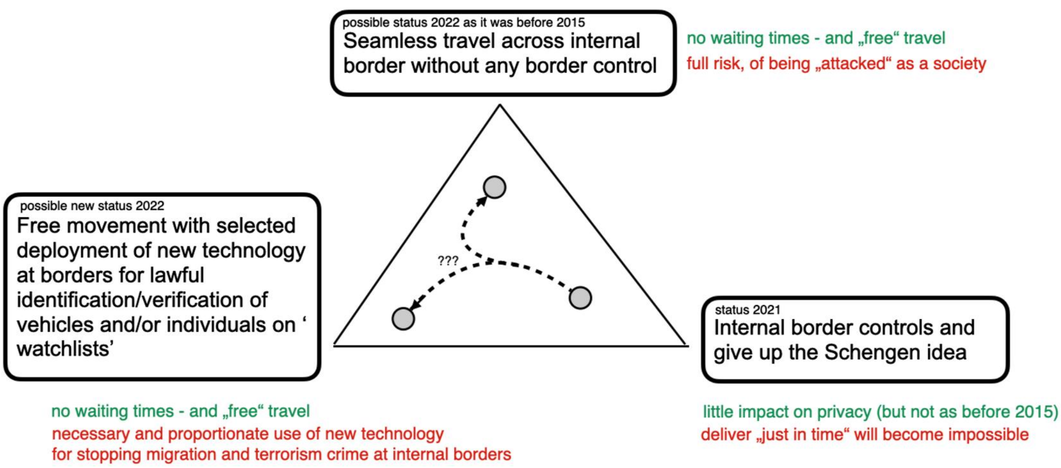

FIGURE 2 Tracking technology versus loss of privacy versus long transaction-time in border control.

pandemic cannot be solely addressed from a technical perspective. The use of biometric technologies to re-establish the freedom to move within the Schengen area raises privacy, ethical, and societal issues (see Section 8 for more details). From a legal perspective, not only should a legal analysis on the necessity and legitimacy to use biometric technologies in these specific contexts be carried out, but each biometric solution should also be preceded by an impact assessment on individuals' rights and freedoms. This should include regulation of all biometric technology beyond data privacy regulations; specifically, the certification, including continuous monitoring, of the technology for its intended use case in the target environment. Finally, using biometric technologies in the context of terrorist threats is not similar, in terms of necessity and proportionality, to using them in the context of a pandemic threat. These purposes need to be considered separately.

The selection of technologies and issues presented in this position paper are based on the academic and industrial experience of the European Association for Biometrics (EAB) members who contributed to the paper. We are convinced that suggested concepts have the potential for being developed and deployed. Prior to a deployment, intensive testing scenario and operational testing with the involvement of relevant authorities would be required.

1.1 | Legal constraints and related considerations

This position paper provides insights on biometric solutions based on different biometric characteristics and other (computer vision) technologies that the European Commission could consider. However, it should be preceded by legal advice on the impacts of such technologies on individuals' rights and freedoms (including the potentially severe effect of these solutions on the freedom to move within the Schengen area). Besides, the paper does not prejudge the legality, necessity, proportionality, and acceptability of these technologies.

The technical propositions described below comprise generally the collection and the use of one or another type of biometric data from individuals. While using such data offers opportunities, including for travelling and free movement, biometric data use in the border control context also poses risks to fundamental rights guaranteed in the EU Charter of Fundamental Rights, including the right to human dignity and to integrity, the right to privacy and data protection, and to non-discrimination [4]. This is reconfirmed in the EU's Fundamental Rights Agency's report Under watchful eyes (2018). Thus, prior to any deployment, one must assess whether any additional biometric data collection/use interferes with such rights, and whether it is strictly necessary. This requires more than 'being desirable' or even 'reasonable'. In some cases, there will be no pressing social need for biometric data collection/use, for example, to bind vaccination/test/recovery certificates to a person, if and because standardised certificates are issued by each member state (MS) and collaboration is guaranteed over a trusted digital network operated by the MS and the Commission, allowing cross-border verification of the validity thereof [5]. The strict necessity shall also be questioned for example, if terrorism attacks or threats are decreasing or if this could lead to constant surveillance. Furthermore, this test requires also that the biometric data shall be effective for reaching the objective while not being replaceable by less harmful means. If all these conditions are fulfilled, the proportionality of the measure is assured, by weighting the competing interests. In other words, and foremost, a thorough impact assessment on fundamental rights and of the strict necessity and proportionality is required ex ante and is essential. In addition to this, the applicable data protection regulation shall be respected as well, as well as ethical and societal concerns being taken into account.

The technical propositions described below will be embedded in existing or new information technology and management infrastructures with information about individuals, whether asylum seekers, citizens of countries belonging to the Schengen area or Third Country Nationals (TCN). It will be essential to determine from the beginning which public/private bodies and entities shall be responsible and take control (also as data controllers), what the precise objectives and purposes are of the collection and use of the personal data (purpose specification principle), which personal data is needed while respecting data minimisation and which entities need access.

The different options for the reestablishment of smooth travel within and across the Schengen zone described by this study require careful assessment from legislative, business and technical perspective. Indeed, while the existing regulations such as the Entry/Exit System (EES) - Regulation (EU) 2017/2226 [6], the Schengen Information System (SISII) - Regulation (EC) No 1987/2006 [7] and Interoperability - Regulation (EU) 2019/817 [8] with their respective implementing acts define the legal boundaries for technologies and processes to be used, several potential options proposed by this study may result in major impacts on the existing central and national solutions (infrastructure, facility layouts, national processes) in place. Therefore, assessing the options based on their level of complexity and expected implementation timeline is of utmost importance.

1. Category 1 - short term goals (3–9 months):
    - Solutions fitting the existing regulations and achievable in short terms with the existing infrastructure and other national constraints.
2. Category 2 – medium term goals (9–24 months):
    - Solutions complying with the regulations in force but requiring amendments to the related implementing and/or delegating acts, and/or
    - Solutions requiring moderate level investments to either or both the national and/or the central EU systems/infrastructure. These solutions may require exceptional budget allocation and additional resources for unforeseen projects.
3. Category 3 – long term goals (over 24 months):
    - Solutions requiring changes to the existing regulations and related implemented acts, and/or

- Solutions with major impacts on either or both national and central side, requiring preliminary pilots, proof of concepts, national and central call for tenders, infusion of high budget and resources.
- Long-term goals can be associated with a high risk, as, for example, in the case that an impact analysis may even prevent deployment. In such cases any specifically suggested technology option may not be viable.

1.2 | Expectations

The elimination of the current border controls and the facilitation of free travel in the Schengen area in a post-pandemic era depends i) on a secure and reliable identification of the traveller (based on the integrity of his or her documented identity) and ii) on the reliable and secure establishment of his or her health status. Both objectives require state-of-the art, secure and interoperable documentation (either in physical or digital form factor) as well as trusted data sources delivering the base data for this documentation (e.g. secure breeder documents such as birth certificates as the foundation of EU passports and ID cards [9], trusted national health infrastructures as the source for standardised heath related proofs). If these interoperable documentations are securely issued by the Member States and subsequently validated by applications using advanced and privacy-preserving technologies in all Member States, free and secure travel in the Schengen area will return.

2 | REASONS FOR CURRENT BORDER CONTROL AND ITS PURPOSE

Diverse reasons exist that have motivated member states over the last 6 years, to depart from the objectives of the Schengen treaty and effectively re-establish internal border control. Such function is normally applied at external borders, to facilitate legitimate trade and travel. However, some Member States now deal with other processes at internal borders that would normally be conducted only at external borders. Some have even closed the border for non-nationals. Despite the legal commitments of the treaty the de-facto status of new control or closure is justified with exceptions, which were declared as temporary but turned to be de-facto permanent for several years. The technology described in the sub-sequent sections may not serve all the reasons and in consequence a deployment of technology will not avoid internal border control, if other reasons prevail. Wherever possible we will refer with proposed concepts to one of the three following reasons:

2.1 | Migration

The interstate wars and the civil wars in the Middle-East region and in Africa in the last 2 decades impacted a strong increase of refugees moving over the Mediterranean and the Balkan route to the Schengen area. These streams were associated in parts with tragic maritime salvage. While a legal regulation for the country responsible for the asylum application was established in 2013 with the Dublin regulation [10] the massive uncontrolled arrival of migrants and asylum seekers in 2015 and thereafter put a strain on many Member States. European stakeholders have requested a distribution of asylum seekers based on the principle of solidarity and shared responsibility, which led to the revision of the Dublin regulation in 2020. However, the evolving situation has caused the introduction of new controls.

2.2 | Terror threats

While the European culture was formed based on tolerance and the respect of different political or religious opinions, the last decades led to an increase of acts of terror conducted by individuals or criminal networks. The tragic incidents as in Paris, Brussels, Berlin, Nice and recently Vienna are examples. Actors are in most cases citizens/residents of the attack country. These terror attacks were the reason for Members States to establish border control as pro-active and/or re-active measure.

2.3 | Pandemic threats

The COVID-19 spread since early 2020 reached the Member States unprepared. Public health authorities must enforce regulations for citizens and TCN. In our global world the only effective countermeasure is vaccinating the population and to include sufficient identity binding in each step of the process: vaccination, vaccination certificate generation, and authentication that the vaccination certificate belongs to the presenter. Member States may reintroduce temporary border controls at internal borders, if justified for reasons of public policy or internal security. In an extremely critical situation, a Member State can identify a need to reintroduce public health policies that affect citizens and visitors internally and at border control points as a reaction to the risk posed by a contagious disease. While the development of effective vaccination was conducted in record time, Member States indeed reduced the risk for their own population by not only controlling travellers entering the Schengen area but also conducting COVID-19 testing at internal borders and eventually even closing the borders for non-nationals. What was lacking in most COVID-19 credentials, including the EU Digital COVID Certificate [11], was identity binding.

Analysing the above reasons for border we can identify three purposes of the border control:

1) limit the migration/follow the flow of migrants and asylum seekers
2) detect and prevent terrorism threats/support after-event forensic investigations
3) limit the spread of pandemic diseases.

While seeking for technology that can facilitate again free passenger journey without border control, we must therefore identify, which of our suggested technologies can address what purpose in addition to the overall intrinsic purpose, namely facilitating free travel. In addition, our suggestions are addressing two meta-goals

4) augmenting processes with privacy enhancing technology
5) defining more robust biometric capture technology with enhanced security by Presentation Attack Detection and Morphing Attack Detection (MAD), as appropriated, in an attempt to mitigate identity fraud.

We must anticipate that the pressure behind migration will increase with the climate change, which will may result in the long term regions in Africa to become uninhabitable, yet no technology described in this paper can reduce said pressure. Neither can technology reduce the motivation of individuals from joining violent radicalisation resulting in acts of terror. On the contrary – distribution of radical opinions is spread via social media – an attack vector that did not exist 20 years ago. Only a political agenda leading to solidarity in a European society shaped by diversity solidarity based on solidarity is tautological can be of help.

3 | USE CASES OF CONTROL MEASURES

When travelling in the Schengen area and when departing/arriving at airports, seaports, railways station or bus station, comprising the following main use cases must be distinguished:

3.1 | Facilitating the passenger journey at airport

Passenger journey currently starts at airport when presenting for the first time at the self-check-in or baggage drop kiosk. Upon presenting a booking QR-code (mobile application or printed booking), passenger then presents biometric passport: in a recommended embodiment, a 3D facial biometric enrolment is performed and a live 2D picture is extracted to be verified against the biometric passport picture. The facial biometric hash is then stored in the mobile application of the Passenger or contained in the printed QR-code of the boarding pass. Passenger can then display or present the QR-code at the border (in that specific case, presenting the biometric passport only would be the main scenario), access kiosks in the connecting flights area, airport lounges, boarding gate, special luggage zone, land border or exit the gate. In case of using a mobile application, the biometric pseudonymous identifier [12], will be securely stored and will be reused by the passenger for further travels, regardless of the operator, airport or EU country of residence. Note that in case of a printed QR-code, the QR-code containing the enrolment data will be valid only for one roundtrip travel. Of course, QR-code shall be digitally signed.

3.2 | Facilitating the passenger journey at the railway station, sea ports, bus station

Similarly, to the airport use case, passengers travelling by train can present a European ID-card or passport at the check-in kiosk and then perform a facial biometric enrolment resulting in a biometric reference, which will also be stored either in the mobile phone of the passenger or printed out in form of a QR-code ticket. Passengers can then present the QR-code at the platform kiosk to access the train. Like for the airport use case, passenger won't have to go to the check-in kiosk to enrol for the next trip (or return trip) as long as a mobile application is being used.

3.3 | Facilitating the passenger journey by car

When the Schengen area was established border control points on highways and motorways disappeared and travelling by car became a more pleasant and more time efficient experience. The recent experience in the COVID-19 and migration crisis was that control points were re-introduced leading to stops, build-up of lengthy queues and potentially waiting times at the border of up to several hours at places, where previously a seamless transition without any stops was possible.

3.4 | Anticipating/detecting terror

Verifying the identity of a driver is one of the means that can be used to anticipate/limit possible terrorist attacks. Upon arriving at the rental location, passengers will present at the check-in kiosk, and follow the same registration flow as the airport use case (additionally presenting their driving licence). As a first step, trucks, vans or pick-ups can be equipped with the same technologies mentioned before (e.g. a QR-code reader or Bluetooth Low Energy reader for their mobile wallet and a 3D camera installed in the driver cabin). To start the car, the driver registered in the rental contract and presented at check-in must be the one on the driver's seat. Continuous and passive facial verification can be performed during the travel: if after 1 min, there is a different person driving, the car can automatically raise an alarm to the rental operator and indicate a change of driver.

3.5 | Verifying EU citizens in quarantine

At airport, railway station, bus station or seaport, passenger shows QR-code to land border or exit gate at arrival. If travel passenger ID and vaccination passport ID have been linked, land border gate can verify if you should be placed in quarantine or not (vaccinated, polymerase chain reaction [PCR] test is negative …). If authorities want to verify the identity of the passenger placed in quarantine, police can visit you at the hotel, use an autonomous tablet to read your travel QR-code and vaccination QR-code. Tablet can be eventually be equipped with a camera to double-check your identity.

Success criteria for these use cases are:

- User Experience
- Inclusivity
- Security Levels
- Interoperability
- Data Privacy & Protection Compliance
- Quick Roll-Out
- Costs

4 | SEAMLESS AND ROBUST BIOMETRIC BORDER CONTROL

Innovative biometric recognition, proposed in the next subsections, requires either

- local storage of biometric reference data (e.g. face images, finger images) on personal devices or Machine-Readable Travel Documents and the biometric verification WITH Schengen internal border control points, as illustrated in Figure 3.

or

- central/national storage of biometric reference data in an identification application WITHOUT Schengen internal physical border control points but with a biometrically-enabled virtual control using sensors at a distance, as shown in Figure 4. Such a system will retain and act on data allowed by current legislation for individuals who are legally entered on relevant watchlists (e.g. all suspect terrorist or open trace face images in Europol/all migrants in Eurodac/missing persons in Europol/politically exposed person [PEP], …). Moreover, the Schengen Information System provides authorities with information on people who may have been involved in a serious crime; who may not have the right to enter or stay in the Schengen area; whose identity has been misused; who are required to assist in judicial procedures; who are missing (both adults and minors) [13]. If a data subject is not on a relevant list, then the biometric and associated data are NOT retained and may be immediately deleted. The infrastructure must reliably destroy all data that does not relate to watchlist entries and such systems must be trusted to include necessary safeguard mechanisms by means of certification.

With the suggested measures for seamless and robust biometric border control we will observe a shift from physical border control with inspecting officers to an electronic check (e.g. remote biometric sensors will allow recognition on the move). Yet the principle of a virtual border control will remain. The electronic checkpoint may also flag those who may pose an infection threat based on central records and sensor data. But there is no need to record and track those who are not on any watch list or pose a threat, thus ensuring the privacy and rights of the vast majority of the travellers.

4.1 | Face recognition

A contact-less technology to authenticate (1 to 1 comparison) or to identify (1 to many comparisons) an individual from a face image. During authentication a probe image is compared

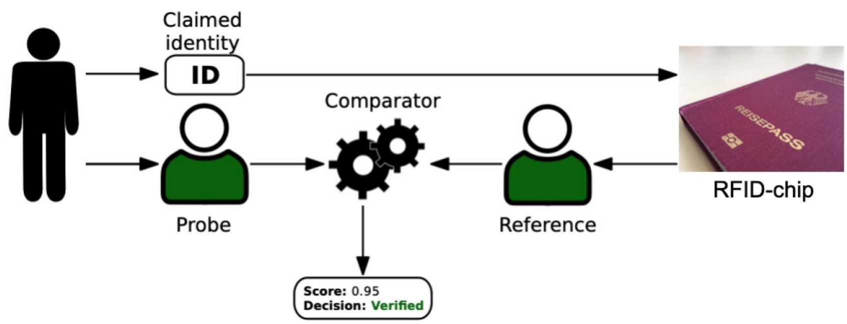

FIGURE 3 Border control with some biometric verification – currently at some internal Schengen borders.

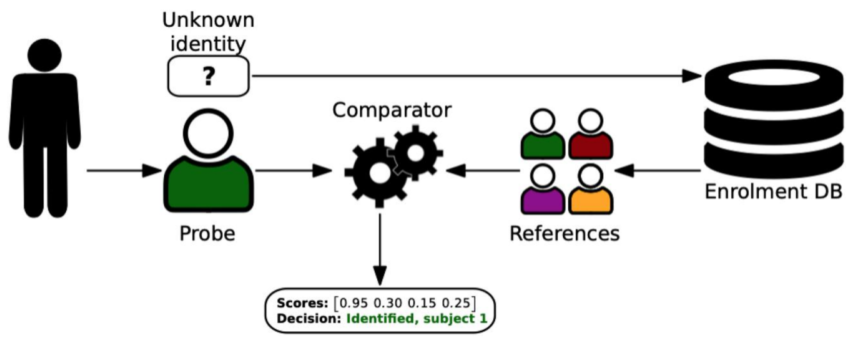

FIGURE 4 Electronic border control at a distance with biometric identification.

to a reference image from a claimed identity. During identification a probe image is compared to a list (e.g. watchlist) of reference images (e.g. video surveillance). In the vast majority of applications, probes and references are from the same domain (i.e. the visual spectra aka. red green blue [RGB]). However, face recognition can also be performed when probes and references are from different spectra (e.g. near-infrared, 3D or Thermal)—this is referred to as heterogenous face recognition [14]. This is of particular interest when probe face images are captured with novel sensing technologies deployed for a dual use, for instance a thermal camera deployed in an airport for temperature screening (to detect a symptom of an infectious disease) can also be used for face recognition against a passport face photograph.

Face recognition is, amongst others, vulnerable to occlusions. Facial masks or coverings have long been used terrorists to hide their identity when committing crimes. According to National Institute of Standards and Technology (NIST) recent evaluation [15], it was observed that the algorithm accuracy with masked faces declined substantially across all algorithms. Unsurprisingly, the authors further observed that the more of the nose a mask covers, the lower the algorithm's accuracy.

For 1:1 comparison, based on NIST's findings, it is recommended that whenever possible, a face mask or covering should be removed to allow a face recognition system to operate normally. When this is not possible, a higher false rejection rate (FRR) is expected. By adjusting the threshold appropriate, the FRR can be reduced; however, this is done at the expense of an increased false acceptance rate. Since each face recognition may behave differently, it is advisable that the system is subject to systematic testing to inform the trade-off that is deemed acceptable.

For face video surveillance, the system must operate with face masks and coverings, thus reducing its effectiveness. A higher false alarm rate and miss detection rate are expected. Alternative imaging solutions based on thermal or infrared red imaging could be considered; but these remain active research topics.

In addition to face biometrics, alternative biometric approaches such as iris recognition using mobile devices with visible light, periocular recognition (i.e. features around the eyes), soft biometrics such as age, gender, ethnicity as complementary features, and voice biometrics can be considered [16]. These modalities are considered in the context of using mobile devices—hence mobile biometrics, which are important solutions for law enforcement officers who need to verify people's identity in the field.

4.2 | Iris and periocular recognition on the move at a distance

Partial faces can be expected in unconstrained environments, such as distant or on-the-move capture processes, but also in controlled ones due to the use of masks. The negative effect of masks is shown in the NIST Face Recognition Vendor Test (FRVT) [15] with >100 identity recognition algorithms which, after more than a year of pandemic, still yield higher error rates. The ocular area, by itself, holds powerful keys of identity [17], soft-biometrics [18], or expression [19], which motivates their use as a stand-alone biometric modality. Also, capturing the periocular region requires less cooperation than the entire face or the iris texture, so it is suitable for unconstrained scenarios or masks.

4.3 | Soft biometric recognition and demographic differentials

In recent years soft-biometrics, including demographic attributes (sex, ethnicity, age), are receiving attention due to their permanence and a relative degree of distinctiveness [20 21]. At the same time the perceived and measurable impact of demographic factors on biometric recognition accuracy is a concern. In some countries, for example, bans or moratoria have been imposed on biometric recognition technology because recognition accuracy for a specific demographic group was feared to be insufficient. As a result, various public and private sector entities have initiated performance assessments to quantify the effects of demographic differentials on recognition performance. NIST, for example, has performed an analysis to measure the relative impact of these characteristics on various face recognition systems with their results published in NIST Interagency Report (NISTIR) 82802 [22].

However, in real-world scenarios such as distant acquisition [23] or partial face view [18], demographic attributes can be retrieved even without active cooperation. In such unconstrained scenarios where a main modality (e.g. face recognition) may struggle, these attributes can help to improve biometric recognition by complementing the main modality [24]. Demographic attributes also have applicability in other tasks of interest for this paper, such as continuous user verification after initial authentication with a stronger modality that demands cooperation, or search of individuals in video data fulfilling certain attributes.

4.4 | Contactless finger- and vein recognition

Hygiene concerns have increased societal resistance to the use of contact-based sensors. These concerns have in turn fuelled research efforts in 2D or 3D contactless fingerprint recognition systems. Both the capture and processing of fingerprints must usually be adapted to contactless capture processes, before traditional minutiae extractors and comparators can be used. On the positive side, fingerprint images acquired using contactless devices do not exhibit the deformations caused by pressing the finger onto a surface that characterize images acquired from contact-based devices. 4/5-Finger acquisition systems are an attractive way for fast and convenient capture.

Hand-vein biometric systems (i.e. palm vein recognition) are mostly operated in contactless-manner nowadays (e.g. in laptop or ATM authentication) while (commercial) finger vein recognition typically relies on a contact-based approach. Only recently, some contactless finger-vein systems have also been designed and tested in a controlled environment (e.g. Kuzu et al. [25]).

In order to facilitate mobile border control (e.g. in trains), there are smartphone apps on the market, which claim to be able to capture vein images from the hand without the need for extra hardware [26].

4.5 | Multimodal contactless biometric corridor

This idea aims to introduce a biometric corridor for travellers (Airports, Train stations, bus stations etc.) to achieve reliable, trustworthy and seamless authentication. Entering the biometric corridor may be reserved to certain categories of travellers (depending on the crossing point), who must enter it through a portal verifying specific electronic ID (and health) credentials to grant them access to the corridor. The multimodal biometric corridor is equipped with several cameras located at different angles and the passport reader. Travellers can scan their passport and pass through the multimodal biometric corridor to capture multimodal biometric characteristics not limiting to face, periocular, iris-on-move and gait. The final authentication decision can be reached based on combining the individual decision from the biometric characteristics. Such corridors can be equipped with multispectral cameras that improve the verification performance by introducing the robustness to the environmental changes of the lighting. Further the sensors can be used to detect Presentation attacks (PA). Finally, the 3D cameras can also be accommodated to compensate for the pose variation issues and a potential negative impact of recognition performance.

Assuring the higher recognition accuracy can be reached by combining information from for example, contactless iris, contactless fingerprint and palmprint, finger-vein/palm-vein, and the face [27 28]. Sequential fusion [29] may reduce the full cooperation of the traveller and maximise the authentication probability [30]. This will provide the traveller with an increasing probability of passing the authentication stage and discouraging attackers and impostors from other people impersonation or to avoid recognition. Multi-modal biometrics have been shown on average to be more robust to PA and constitute an excellent deterrent [31]. Note that multi-sensor-based implementation of multi-modal biometrics does not necessarily increase cost and complexity and neither the transaction time, as all capture processes take place simultaneously. Furthermore, providing effective artefacts for contactless biometrics, such as iris, finger-vein, and palm-vein, requires high specialisation and motivation [32]. Finally, they can avoid touching multiple capture devices' surfaces, a matter of great help in facilitating travelling in pandemic times. Other general hygiene aspects and best practices are further discussed in Section 8.

4.6 | Attack detection

Presentation attacks are attempts to subvert the system using a fake artefact (such as gummy fingers) and pose a severe threat to the security of biometric systems [33]. This is especially critical in unattended scenarios, making necessary automatic techniques to detect PA. Solutions to distinguish between a bona fide subject in front of the capture device and artefacts include multispectral acquisition [34], analysis of static properties of the image (e.g. skin pores, light reflections, image artefacts, texture), or dynamic properties (e.g. challenges by lip-reading, video captchas [35], or voluntary/unvoluntary actions like blinking, gazing, smiling etc.) [36 37]. It is recommended to integrate sensors in the capture device that can clearly distinguish artefacts from human skin [38]. The vulnerability of face recognition systems to Morphing Attacks (MA) and detection of such attacks is also receiving great attention [39]. In MA, the face image contained in the e-passport is a morphed image composed by combination of two parent images. An e-passport with a morphed face image can be used by both subjects since the morphed face image can be verified against both of them, but only one identity (the name written in the passport) would be recorded in the system log. As research on MAD is progressing, countermeasures in terms of robust detection mechanisms should be integrated [40].

4.7 | Self-registration

Self-registration can take place before and/or after border crossing with face recognition. In that case travellers could enrol and verify their travel document before starting their journey, and could be prompted for additional responses after crossing of Schengen internal borders. This could be combined with face recognition control points (e.g. airport). If the traveller opted-in for self-control before and after crossing, authorities could use beacon trackers to verify in a seamless manner that travellers have their enrolled phone with them. A pre-enrolled traveller would need to drive somewhat slower in a specific lane at the border but would not need to stop unless flagged. Such self-registration technology supports the sharing of cryptographically verifiable information in a secure, privacy enhancing manner such that a traveller could provide trusted, verifiable credentials prior to travel in ways that border control authorities can validate and pre-process prior to physically verifying the traveller's identity at the border control point.

4.8 | Privacy preserving solutions

Current solutions for biometric deployment do operate with protected (i.e. encrypted) biometric databases, but not sufficiently protected to guarantee privacy preservation even in case of data loss and the used encryption scheme being broken. This is highly problematic, as we have seen many attacks against biometric systems being facilitated by compromised biometric template databases (e.g. inversion attacks & PA to name two prominent examples). In order to achieve trust in public perception, privacy preserving technologies should be implemented in the early stage of the design of a biometric based system. This is reflected in the need to design privacy compliant biometric systems architectures and to design privacy enhancing techniques for the protection of biometric templates.

From an architectural point of view, templates can be stored in a distributed or centralised manner. Of course, a distributed way to store biometric templates (on tokens like smartcards, ID-documents) is clearly better in terms of privacy preservation, as there is no single point of attack. As for the privacy enhancing techniques, cancellable biometrics come probably closest to what in public is considered to be privacy preserving, as biometric templates can be changed in case of compromise or in case of regular security updates just like we are used to do when changing passwords. As an alternative countermeasure homomorphic encryption is a promising protection mechanism [41]. Other important security and privacy questions do arise in case personal smartphones are considered to be integrated into an authentication architecture [42 43]. Being untrusted devices per definition, an involvement is certainly problematic. Also, the intense use for private communications makes smartphones a problematic device when it comes to privacy-preserving technology.

For surveillance-based biometric systems the compliance of an operational face recognition system with the international standard (under development) ISO/IEC 9868 "Remote biometric identification systems — Design, development, and audit" will be relevant.

5 | COMPENSATORY MEASURES - PHYSICAL AND SMARTPHONE BOUND SUPPORT

This section proposes measures that are independent from a biometric verification or identification application, but could well be combined with a biometric service.

5.1 | Birth certificates

During the migration crisis the verification of the migrant's identity against breeder documents (such as internationally standardised birth certificates) was not possible. Neither was it possible to have a cross-national verification of the documented information. Subsequently not even a reliable information about the age of many juvenile asylum seekers was available in the processes, operated by member states. The definition of an ISO/IEC standard for birth certificates and the registration of such certificates by a global institution (i.e. United Nations) could on the long range solve such problem. The International Civil Aviation Organisation (ICAO) has identified this need [44]. It has been shown, that such birth certificates can have a biometric link to a persistent biometric characteristic such as the iris or the fingerprint, which does not change over the life time, as illustrated in Figure 5 [45].

The European Standardisation body (i.e. CEN/TC 224/WG 19) is working on secure and interoperable Breeder Documents and incorporating biometric references. This work was initiated on request of the European Commission.

FIGURE 5 Proposed birth certificate from the FIDELITY project [46]. Left: Draft product design. Right: Sizes of barcodes correspond to the approximated storage requirement for the compressed biometric sample.

Currently there are two technical specifications under development:

- CEN TS 17489-2: Data model
- CEN TS 17849-5: Trust establishment and management processes

Part 1 of this multipart standard is published and provides an overview on the envisioned framework [47]. While CEN is a European Standardisation Body, the specifications are probably of broader interest and it is very likely that 17,489 will later be adopted by ISO/IEC under the Vienna agreement.

5.2 | Identity document validation

Identity document validation technology is an umbrella term used to describe various ways of checking the validity of physical identity and travel documents. The checking must be commensurate with its usage. Identity document validation technology performs one or more of the following functionalities:

- Checking that the document is authentic or genuine—that it has not been tampered with, and that is not forged or counterfeited.
- Checking that the document is still valid (i.e. not yet expired).
- Checking that the document holder is its owner by comparing the holder's live face image against the recorded image stored electronically or printed on the physical ID document.
- Checking that the information on card or stored in the barcode is valid. For example, check that the address is valid, and the card holder still lives in the recorded residential address.

5.3 | Digital traveller credential

Specifications for the Digital Traveller Credential (DTC) Physical Component that are currently being drafted, will open-up the possibility to store additional data into the DTC Virtual Component (DTC-VC). This will enable States to issue type-2 DTCs with health information incorporated. Consequently, that would eliminate the need for a separate health certificate.

5.4 | Corona free test certificate and vaccination certificate

In the context of the pandemic, all stakeholders are looking to develop accessible, secure and interoperability solutions that enable the competent authorities, such as issuance and verifier entities to generate and to verify a forgery proof certificate (ex: a QR code) attesting the existence of a valid vaccination certificate, a COVID-19 test result or a proven immunity period. The results in printed and digital versions should be binding to an identity and must respect the data privacy regulation in both cases. Because of the risk of false certificates, but also because of the need to guarantee and to facilitate free movement in the Union, the Commission proposed a framework for initially called Digital Green Certificates [5] and later be termed as EU Digital COVID Certificate [11], which are interoperable and verifiable certificates with information about vaccination, testing and/or recovery. When crossing borders, the signature of the certification authority is checked. Biometric information could in itself be useful for binding the certificate of the right person when presenting the certificate at the borders. Yet another option is a traveller's mobile application with this private data about health which the officer at the border can read only when confirming the request on the mobile phone.

Governments identify accredited laboratories and provide them with multi-factor authentication to access government platform and generate Digital Seal for signing health certificates. By doing so government set-up trusted ecosystem within country and could use ICAO Visible Digital Seal (VDS) standard for international recognition of the health certificates. International Civil Aviation Organisation VDS is an internationally recognised standard of a 2D bar code for sealing health certificates for travel-related purposes. The VDS is signed using a Country Signing Certification Authority Public Key Infrastructure (PKI), which is already used for signing ePassports. A dedicated PKI can also be developed for health purposes. Therefore, the secure exchange of public keys can be done using a Public Key Directory either operated by EU or by WHO. Based on privacy by design approach, the health data are not required to be stored in any central database. The traveller is the only holder of his medical results and can select which data will be presented to the verifier for the verification. For the travel within Schengen area, a traveller could display ICAO VDS and verifier should access only to minimum data such as name, surname, passport number, vaccination/PCR/immunity result (e.g. green = ok, red = not ok).

5.5 | FIDO2 and Public Key Infrastructure

FIDO2 is a specification proposed by the Fast IDentity Online (FIDO) Alliance which enables any Relying Party (RP) such as government agencies and commerce to authenticate users securely without using passwords. Instead, they are replaced by the PKI protocol. When a user first enrols themselves, a cryptographic key-pair is created, which consists of a private and a public key. The private key is kept secret and remains on the device, whereas the public key is transmitted to the RP, which stores the key in the FIDO server backend. Leveraging on strong industrial supports, FIDO has the potential tool to allow users to store eMRTD, eID or ePassport using a smartphone that they already carry with them anyway. In a white paper [48] the FIDO Alliance explains how FIDO2 can support the deployment of electronic identity tokens in accordance with eIDAS article 8. The technology is appealing because of the following reasons:

- Popular browsers have already implemented WebAuthn
- Biometrics used in eID can be readily integrated with FIDO
- Biometrics data required for authentication never leaves the device (it is decentralised)
- The users are in control of their data

6 | COMPENSATORY MEASURES—SMARTPHONE TRACKING OF SUSPECTS

A technology that can address the terror threat (described in Section 2) and only that threat is the recognition of personal devices and the tracking thereof. This approach must be considered as highly privacy invasive and it is questionable whether such data use under the European legislation is proportional. The idea of the approach is to derive from the hardware of the device and from the SIM-card a pseudonymous device identifier. For smartphone users that are known to have a terroristic motivation or be closely related to known extremists, the device identifier can be registered in a central system. In support of forensic pro-active actions of police operations such device identifiers could be tracked via the cell registration and the physical approaching of the device to a critical infrastructure (parliament, nuclear power plant etc.) could raise an alarm and trigger police pro-active actions.

6.1 | Biometric link of data subject to a smartphone

Tracking of a smartphone is of limited benefit, if the device is used by multiple individuals. Biometric recognition can establish a strong link between a data subject and the device. Such a link can be based on biological characteristics (e.g. capturing face, periocular and ear) or behavioural characteristics (e.g. voice, gait, typing etc.). Research has shown that recognition accuracy of such methods is sufficiently good for a verification approach needed in this context [17 49 50 51 52]. Activating such biometric recognition in a device of a terrorist suspect remains a challenge and poses legal questions in the absence of consent.

The widespread availability of sensors such as accelerometers and gyroscopes in smartphones, and more recently inclinometers, has opened the way for the development of gait monitoring algorithms. The introduction of deep learning neural network techniques into this field has made it possible to achieve sufficiently good verification accuracy in biometric authentication of individuals based on the way they move, which is now comparable to the results achieved by the best biometric algorithms [53 54]. One should note that such accelerometer-based biometrics is not competing with face recognition, as it is a way of unobtrusive biometric recognition that can link the smartphone to the owner and can stabilise the verification result over a series of time windows. It should be considered as a complementary technology to face recognition and thus not competing with the security model on which a face recognition model can be established.

Another technique to link data subject to smartphones and does not require physical contact with the user is auricle shape recognition. The smartphone front camera is used to acquire an image of the ear as the handset is brought closer to the head. Also, such an image can be acquired using external cameras. This technique, to which machine learning has also been introduced, is characterised by high efficiency while being immune to factors that hinder facial recognition, such as make-up, facial hair, and anti-viral masks.

7 | COMPENSATORY MEASURES - COMPUTER VISION FOR VEHICLE TRACKING AND BIOMETRIC VEHICLE BINDING

7.1 | Number plate recognition

In the Netherlands, a pilot, then known as @Migo-Boras, was set up around 2010 [55], patrolling the borders with Belgium and Germany in an area of 20 km by mobile and fixed cameras on highways, checking car licence plates against multiple police databases aiming to stop illegal immigrants and criminals. The project, which came after a similar initiative in Denmark (which was in the meantime stopped) was criticised as it was considered as re-establishing border control and leading to surveillance. Thereafter, the project was somehow modified, renamed as 'Mobile Surveillance Security (MTV)' (MTV) and continued in 2011 for then only about 6 h a day, and maximum 90 h per month. Research in close collaboration with the border police ('Marechaussee') indicated that there was a shift in use from migration control to combating crime and that the impact of the technology on the decision taken during MTV checks of the border police overall remained limited since 'the information they receive is often not specific enough and they see little added value in the intelligent camera system' [56].

7.2 | Car and subject tracking

Biometrics and computer vision in combination can contribute to free movements effectively. Vehicles (via drivers) or travellers, can send information on traveller(s), vehicle and/or cargo details in advance via mobile apps. Later, at the border, cameras can detect and verify identities of travellers and cars while checking for PA or counterfeited identity documents with minimal time loss. To verify identities, different modalities can be applicable (Section 4) depending on the concrete scenario, such as: face recognition (collaborative), iris/periocular at a distance (e.g. biometric corridor, or when masks are in use), fingerprint or finger vein (both contact and contactless). Regarding vehicles and cargo, cameras can automatically 1) recognise plate, and 2) recognise "mechanical properties" of the vehicle, and verify the outcome with what the registration plate information and information submitted in advance is claiming, for example, on brand, unloaded weight, size, brand, colour etc.

7.3 | Detecting attacks with large goods vehicles

The consequences of kidnapping a vehicle could be mitigated by knowing the identity of passengers continuously, initiating an alarm if it is driven by a non-eligible driver, or if there is a violent act inside. Continuous biometric identification can be achieved without active collaboration via dynamic ocular and mouth region information, including visual speech and facial expressions (without audio) [17 57] As a pro-active measure face and periocular recognition will prevent future terror threats like the Berlin or Nice incident. The concept suggests to establish a strong biometric link between an aeroplane or truck and the authorised pilot or driver. This specifically relevant, if such large-scale and large goods vehicle (i.e. larger than 3.5 tons) is transporting valuable goods (humans) or dangerous goods (chemicals, nuclear material etc.). With little modification of the vehicle control units, the biometric system can stop the mobility of the massive vehicle, if the biometric verification of the enrolled pilot/driver fails [58]. Also, by surveillance, heavy unexpected vehicles or with an abnormal speed close to critical areas (e.g. a nuclear power-plant or pedestrianised streets) can be detected, triggering early alerts before they reach the area.

8 | PRIVACY, ETHICAL, AND SOCIETAL CONSIDERATIONS

Biometric technologies are one of the management tools used to control the external borders of the Schengen area and ensure security ('to fight against terrorism and serious crime', see for instance the Council of the EU, 'Strengthening the EU's external borders'). But their use inside the Schengen area is a novelty as this does concern third-country nationals and EU citizens and residents. Such an extension for the sake of internal security should be subject to a democratic debate. From a societal perspective, using biometric technologies to 'secure' the internal Schengen area could have the paradoxical effect of recreating invisible borders with the risk of constant surveillance. Their use needs to be balanced with and assessed against their impacts on individuals' fundamental rights. Due to their characteristics and specific link to an individual, biometric data are not only sensitive data, but they also have the ability to reveal sensitive information (such as ethnicity or health condition). Yet, individuals might prefer to conceal these pieces of information, which could be used to discriminate against them. Besides the rights to privacy and data protection, biometric technologies might affect the right to non-discrimination, have a chilling effect on the freedom to move and on the freedom of assembly, and potentially infringe the EU general principle of proportionality. According to that principle, public authorities need to strike a balance between the purpose of their action and the means they use to reach it. They also need to balance the collective security against the protection of fundamental rights.

8.1 | Demographic fairness

An essential consideration in all deployments of biometric systems is that, in as far as possible, operational performance in terms of accuracy is not biased towards a particular population subgroup, be that ethnicity, disability, age rage or other characteristic. It is vital therefore that developers and implementors ensure that systems are proven on a representative population with respect to the final deployment environment, including with a juvenile population if operationally appropriate. In order to achieve fairness, it is important that representative training datasets become available, which is currently a blocking issue for both Member States and eu-LISA.[1] Likewise, consideration need be given to acceptability of a proposed solution across the widest possible population. Characteristics such as physical and mental disabilities, and cultural considerations (for example, in clothing) may preclude individual subjects from interacting (successfully or otherwise) with a biometric system. Implementations should make allowances for population characteristics with methods such as adaptive thresholds or utilising multiple modalities. In doing so it is important, however, that the security afforded by an implementation is not compromised.

8.2 | Security by design

The acceptability of biometrics systems would greatly increase if people and institutions were aware that the acquired facilities were much more relevant than the risks connected to the invasiveness of the authentication procedure. To this goal, the security-by-design paradigm, which was developed in software engineering [59], gives the basis of an "intrinsically secure" system, where the issues involving vulnerabilities, internal or external attacks, by physical or virtual means, are taken into account during the architecture design phase. In particular, the human-in-the-loop possible errors or traps exhibit a crucial role in people trusting [60]. The proposed paradigm can be easily adopted in biometric systems that must pass as good solutions and not as bridges to further and crucial security breaches. In other words, we believe that encouraging the formalisation and development of the "secure-by-design" paradigm in biometrics by academies and companies may lead to a generation of authentication systems fully trusted by institutions and common people.

8.3 | Paper-based credentials

In addition to accessibility, there needs to be further consideration on the inclusive role digital devices play. Although there is no doubt that mobile phones boost tremendously the adoption of digital identity and its related services, the identity of a person cannot be restricted to a single device approach or

[1] European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.

connectivity availabilities. Therefore, in order to be inclusive at social and technical levels and not dependent on contextual environments, other alternatives should be considered such as: paper-based credentials, which could be enhanced with printed privacy respecting biometric link. While paper-based credentials can be faked, forged, or counterfeited, the identity document validation technology as discussed in Section 5 should be considered.

8.4 | Hygienic precaution

Cross-border movements of people must not increase the spread of diseases by pathogens—organisms such as bacteria, viruses, or other microorganisms that can cause diseases. Pathogens can stay on the surfaces of contact-based biometric devices (e.g. finger, finger vein, palm vein and hand geometry capture devices), apparatuses, or furniture including turnstiles and gateways so they can pose significant risks to disease spreading. The following best practices can be recommended for devices and apparatuses used in cross-border scenarios:

- Clean the devices and apparatuses, including their housing enclosures with disinfectants with each use—once before and once after usage.
- Consider using contactless or at-a-distance biometric systems, for example, contactless fingerprint capture devices, or face, iris, and other contactless biometrics.
- Reduce contact time and apply social distancing measures between and among operators and capture subjects.

9 | CONCLUSION

In this position paper a number of technological options have been discussed. Some could be implemented in the short-term while others can only be deployed in the mid- to long-term. We consider short term a period of approximately 1 year, mid-term as approximately 5 years and long-term as approximately 10 years or longer. Some of these options may not be currently compliant with the European data privacy practice and legal framework and may therefore not be suitable for immediate deployment. Table 1 summarises all options and provides an assessment. This summary table was composed with a methodology, which is well known from the ISO/IEC directives [61], according to which contributions from experts were reviewed by the other group members and a consensus was reached in a meeting with disposition of contributions and comments. The options that are outlined are the consequence of the interdependencies and contradicting objectives. Since not all border crossing inspection sites and conditions are the same, it is not possible to define finally which methods are universally right and which are entirely excluded. It is up to the system designers at each (type of) physical sites and authorities to decide this.

Privacy preserving measures as suggested in Section 4.8 should accompany all biometric data processing. Furthermore, it should be noted that many of the technological options discussed and listed in Table 1 are evolving quickly with the potential offered by Artificial Intelligence (AI). Ongoing advances and improved pattern recognition capability for biometric and non-biometric tasks protecting the Schengen area can be expected. However, the progress of AI and the increased deployment of AI-based system can also be considered as risk for the society [62].

Under the assumption that neither a physical nor an electronic border control ("biometric corridor") is desired or could be implemented, then the suggested measures are limited to the following:

- 5.1 Birth certificates and UN based registration as pro-active steps towards United Nations Sustainable Development Goal 16.9 (UN-SDG 16.9)
- 7.3. Preventing attacks with large goods vehicles by on-car prior registration of authorised drivers (pro-active measure) to prevent high-jacking of vehicles.

In addition, if the presence of existing and widespread sensor regional infrastructure (e.g. smart cameras, mobile-network cell) is utilised, the following measures are possible and can support police investigations, and the recorded data being interlinked and correlated in a post-terror evaluation:

- 4.1 3D face recognition for re-active forensic investigations (post-terror incident)
- 4.1 Thermal face recognition for re-active forensic investigations in poor illumination (post-terror incident)
- 4.2 Iris and periocular recognition for re-active forensic investigations under a masked face scenario (post-terror incident)
- 4.3 Soft biometric recognition for re-active forensic investigations (post-terror incident)
- 4.7 Self-registration for travellers as pro-active prevention of un-controlled migration and pandemic spread (voluntarily participation)
- 4.8 Privacy preserving solutions for pseudonymous solutions for infrastructure (i.e. database) implementations
- 6. Smartphone tracking of suspects in a post-terror incident investigation
- 7.1. Number plate recognition as re-active forensic investigations (post-terror incident)

Directly related to technological innovation of biometric systems, and ethical and legal considerations of use, is knowledge and understanding of deployment and operation. Systems will perform sub-optimally if they are not appropriately deployed or operated, or outputs/system decisions are interpreted incorrectly. Training on system design, use and interpretation for stakeholders, including managers, systems designers, procurers, and field officers (amongst others) is vital to ensure both technological accuracy and safeguards for correct and appropriate operation. Several European organisations like eu-LISA, FRONTEX or the EAB have programmes of training and education designed directly to address requests from such stakeholders, covering both fundamental and advanced topics on biometric technology operation, ethical and legal design and emerging solutions.

TABLE 1 Summary of discussed technology.

Section Suggested technology	Time range	Mode	Purpose: addressing	Infra-structure needed	Likely increase of privacy impact (subject to full privacy and data protection impact assessment)
4.1 3D face recognition	Medium term	pro-active and re-active	PAD.	no	Low
4.1 Thermal face recognition	Medium term	pro-active and re-active	PAD. Detect infected in times of pandemic.	no	medium to high
4.2 Iris and periocular recognition	Medium term	pro-active and re-active	PAD-robustness supports corridors	yes	Low
4.3 Soft biometric recognition	Medium term	re-active	Terror	no	Low
4.4 Contactless fingerprint recognition	Short term	pro-active	Pandemic	no	Low
4.4 Contactless vein recognition	Medium term	pro-active	Pandemic	yes	Medium
4.5. Multimodal contactless biometric corridor	Medium term	pro-active	Seamless operation, improved performance	no	Low
4.6 Presentation attack detection	Short term	pro-active	Migration Terror	no	Low
4.6 Morphing attack detection	Long term	pro-active	Migration Terror	no	Low
4.7 Self-registration	Medium term	pro-active	Pandemic Migration	yes	Medium
4.8 Privacy preserving solutions	Medium term	pro-active	PET	yes	Low
5.1 Birth certificates and UN based registration	Long term	pro-active	Migration	yes	Low
5.2 Identity document validation	Short term	pro-active	Migration Terror	yes	Low
5.3. Digital traveller credential	Short term	pro-active	Migration Terror	yes	Low
5.4 Digital Green Certificates	Medium term	pro-active	Pandemic	yes	Medium
5.5. FIDO2 and PKI	Short term	pro-active	PET	yes – establish link to FIDO PKI	Low
6. Smartphone tracking of suspects	Short term	pro-active and re-active	Terror	yes	very high
7.1. Number plate recognition	Short term	pro-active and re-active	Terror	yes	high
7.2. Car and subject tracking	Medium term	pro-active and re-active	Pandemic Terror	yes	high
7.3. Detecting attacks with large goods vehicles	Short term	pro-active	Terror	no	Low

Section – refers to the description in earlier sections of this document.

Time range – of the implementation of discussed technology (short-term, mid-term, long-term).

Mode – serving as pro-active or as re-active measure.

Purpose – indicating the purpose of the control measures addressing a reason for current border control (migration, terror, pandemic) and the meta-goals (privacy enhancing technology PET, enhancing security by PAD).

Infrastructure – does the measures require a (non-existing) local or central infrastructure.

Likely increase of privacy impact – on our European privacy culture (none, low, medium, high, very high). This is based on an ad-hoc discussion and is by no means replacing a full prior privacy and data protection impact assessment, which must be addressed, before any suggested technology is deployed.

Returning to the triangle in Figure 2 it seems that a compromise solution may be needed and possible. Seamless travel, - without tracking of travellers not under suspicion and therefore who present no threat, and with minimum controls such as those to protect the public from the spread of infection and address security threats - seems to be an objective that is hard to achieve. In any case it requires a judicious implementation of technology with full regard to legal safeguards. This position paper does not claim to provide the necessary holistic approach to reach an optimal trade-off between open borders and the maintenance of a high-level of security together with the protection of fundamental rights. However, the intention has been to support the achievement of this objective, bearing in mind the assessment made of the technology options.

Biometrics will continue to have a strong impact on the security of European borders and other governmental and commercial applications. In order to ensure compliance with European Data Protection principles, Privacy Enhancing Technologies that are available should be deployed. As for all technology, biometric technology should be carefully implemented, tested, and certified. A pro-active and cognizant approach could foster awareness among the citizens and policymakers, as well as contribute to minimising potential negative effects and perception of biometric technology and innovation by individuals and society as a whole. The European Commission is encouraged to continue and expand its support for research and development in the field of biometric and privacy-enhancing technologies, industrial follow-ups, the adoption and deployment of ISO/IEC standards as well as its interaction with the EAB which continues to play an important role to foster a shared understanding of security and mobility challenges and their solutions.

AFFILLATIONS

[1]Norwegian University of Science and Technology, Gjøvik, Norway

[2]University of Kent, Canterbury, UK

[3]European Association for Biometrics (EAB), Amsterdam, Netherlands

[4]KU Leuven, Leuven, Belgium

[5]HID, Jena, Germany

[6]European Association for Biometrics, Darmstadt, Germany

[7]European Association for Biometrics, Paris, France

[8]Griaule Unipessoal LDA, Lisbon, Portugal

[9]Halmstad University, Halmstad, Sweden

[10]Accenture, Arlington, USA

[11]Hitachi Europe Limited, Maidenhead, UK

[12]Trust Stamp, Stroud, UK

[13]eu-LISA, Kehl, Germany

[14]Rey Juan Carlos University, Madrid, Spain

[15]Roma Tre University, Roma, Italy

[16]eu-LISA, Tallinn, Estonia

[17]Trust Stamp, Bristol, UK

[18]European Association for Biometrics, Jerusalem, Israel

[19]KIS SAS, Echirolles, France

[20]Gdansk University of Technology, Gdansk, Poland

[21]Telecom SudParis, Evry, France

[22]Brno University of Technology, Brno, Czech Republic

[23]Hochschule Darmstadt, Darmstadt, Germany

[24]SICPA SA, Prilly, Switzerland

[25]Universidad Autonoma de Madrid, Madrid, Spain

[26]Hochschule Ansbach, Ansbach, Germany

[27]Secunet Security Networks AG, Essen, Germany

[28]Vision-Box, Lisbon, Portugal

[29]Idiap Res Institute, Martigny, Switzerland

[30]University of Cagliari, Cagliari, Italy

[31]Idemia, Paris, France

[32]NORIA Onlus, San Vito al Tagliamento, Italy

[33]CLR Labs, Gemenos, France

[34]Telecom T&M SudParis, Paris, France

[35]Trust Stamp, Cheltenham, UK

[36]eu-LISA, Strasbourg, France

[37]OneVisage, Lausanne, Switzerland

[38]BKA, Wiesbaden, Germany

[39]University of Twente, Enschede, Netherlands

[40]Mobai, Gjovik, Norway

[41]European Association for Biometrics, Pirkkala, Finland

[42]European Association for Biometrics, Salzburg, Austria

AUTHOR CONTRIBUTION

Christoph Busch: Supervision. Farzin Deravi: Writing – review & editing. Dinusha Frings: Writing – review & editing. Els Kindt: Writing – review & editing. Ralph Lessmann: Writing – review & editing. Alexander Nouak: Writing – review & editing. Jean Salomon: Writing – review & editing. Mateus Achcar: Writing – review & editing. Fernando Alonso-Fernandez: Writing – review & editing. Daniel Bachenheimer: Writing – review & editing. David Bethell: Writing – review & editing. Josef Bigun: Writing – review & editing. Matthew Brawley: Writing – review & editing. Guido Brockmann: Writing – review & editing. Enrique Cabello: Writing – review & editing. Patrizio Campisi: Writing – review & editing. Aleksandrs Cepilovs: Writing – review & editing. Miles Clee: Writing – review & editing. Mickey Cohen: Writing – review & editing. Christian Croll: Writing – review & editing. Andrzej Czyzewski: Writing – review & editing. Bernadette Dorizzi: Writing – review & editing. Martin Drahansky: Writing – review & editing. Pawel Drozdowski: Writing – review & editing. Catherine Fankhauser: Writing – review & editing. Julian Fierrez (GE): Writing – review & editing. Marta Gomez-Barrero (GE): Writing – review & editing. Georg Hasse: Writing – review & editing. Richard Guest: Writing – review & editing. Ekaterina Komleva: Writing – review & editing. Sebastien Marcel: Writing – review & editing. Gian Luca Marcialis (GE): Writing – review & editing. Laurent Mercier: Writing – review & editing. Emilio Mordini: Writing – review & editing. Stefance Mouille: Writing – review & editing. Pavlina Navratilova: Writing – review & editing. Javier Ortega-Garcia: Writing – review & editing. Dijana Petrovska: Writing – review & editing. Norman Poh: Writing – review & editing. Istvan Racz: Writing – review & editing. Raghavendra Ramachandra (GE): Writing –

review & editing. Christian Rathgeb: Writing – review & editing. Christophe Remillet: Writing – review & editing. Uwe Seidel: Writing – review & editing. Luuk Spreeuwers: Writing – review & editing. Brage Strand: Writing – review & editing. Sirra Toivonen: Writing – review & editing. Andreas Uhl: Writing – review & editing.

CONFLICTS OF INTEREST STATEMENT

The authors declare that no conflict of interest exists in the submission of this manuscript.

DATA AVAILABILITY STATEMENT

Does not apply.

REFERENCES

1. Communication form the Commission to the European Parliament and the Council: A Strategy towards a Fully Functioning and Resilient Schengen Area (2021)
2. European Commission: Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) 2016/399 on a Union Code on the Rules Governing the Movement of Persons across Borders (2021)
3. UK HM Government: National Risk Register (2020)
4. Charter of Fundamental Rights of the European Union, OJ C326, 26.10.2012, pp. 391–407 (2012)
5. Pandemic (Digital Green Certificate) (2021)
6. Nationals (2017)
7. Generation Schengen Information System (SIS II) (2006)
8. Data (2019)
9. CEN/TS PWI: Personal Identification – European Guide for Verification Applications Based on ID Documents (2022)
10. European Union: Country Responsible for Asylum Application (Dublin Regulation) (2020). https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/examination-of-applicants_en
11. European Commission: New Rules on the Validity of EU Digital COVID Certificate and the Coordination of Safe Travel in the EU (2022). https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en
12. ISO/IEC JTC1 SC27 Security techniques: ISO/IEC 24745:2011, Biometric Information Protection (2011)
13. eu-LISA: Schengen Information System II (2022). https://www.eulisa.europa.eu/Publications/Information%20Material/SIS%20II_EN_web.pdf
14. Pereira, T., Anjos, A., Marcel, S.: Heterogeneous face recognition using domain specific units. IEEE TIFS (2018)
15. U.S: NIST Face Recognition Vendor Test
16. Gomez-Barrero, M., et al.: Biometrics in the Era of COVID-19: Challenges and Opportunities. arXiv preprint arXiv:2102.09258 (2021)
17. Alonso-Fernandez, F., Bigun, J.: A survey on periocular biometrics research. arXiv:1810.03360 (2018)
18. Alonso-Fernandez, F., et al.: Cross-sensor periocular biometrics for partial face recognition in a global pandemic: comparative benchmark and novel multialgorithmic approach. Elsevier Information Fusion journal (2022)
19. Alonso-Fernandez, F., Bigun, J., Englund, C.: Expression recognition using the periocular region: a feasibility study. In: Proc. Workshop on Ubiquitous Implicit BIOmetrics and Health Signals Monitoring for Person-Centric Applications, UBIO, in Conjunction with the Intl Conf on Signal Image Technology & Internet Based Systems. SITIS (2018)
20. ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 39794-1:2019, Extensible Biometric Data Interchange Format – Part 1: Framework (2019)
21. Becerra-Riera, F., Morales-Gonzalez, A., Mendez-Vazquez, H.: A survey on facial soft biometrics for video surveillance and forensic applications. Artif. Intell. Rev. 52(2), 1155–1187 (2019). https://doi.org/10.1007/s10462-019-09689-5
22. U.S. NIST Face Recognition Vendor Test: Part 3: Demographic Effects. NISTIR 8280 (2019)
23. Tome, P., et al.: Soft biometrics and their application in person recognition at a distance. In: IEEE Transactions on Information Forensics and Security (2014)
24. Sun, Y., et al.: Demographic analysis from biometric data: achievements, challenges, and new frontiers. In: IEEE Transactions on Pattern Analysis and Machine Intelligence (2018)
25. Kuzu, R.S., et al.: On-the-fly finger-vein-based biometric recognition using deep neural networks. In: IEEE Transactions on Information Forensics and Security (2020)
26. Uhl, A., et al.: Handbook of Vascular Biometrics. Springer (2020)
27. Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics. Springer (2006)
28. H2020 project: BES-6-2015: Border Crossing Points Topic 2: Exploring New Modalities in Biometric-Based Border Checks (2019). http://projectprotect.eu/
29. Fierrez, J., et al.: Multiple classifiers in biometrics. Part 1: fundamentals and review. In: Information Fusion (2018)
30. Marcialis, G.L., Roli, F., Didaci, L.: Personal identity verification by serial fusion of fingerprint and face matchers. In: Pattern Recognition. Elsevier (2009)
31. Biggio, B., et al.: Statistical meta-analysis of presentation attacks for secure multibiometric systems. In: IEEE Trans. On Pattern Analysis and Machine Intelligence. IEEE (2017)
32. Marcel, S., et al.: Handbook of Biometric Anti-spoofing. Springer (2019)
33. CEN/TS PWI: Digital Presentation Attack in Biometric Systems (2021)
34. Tolosana, R., et al.: Biometric presentation attack detection: beyond the visible spectrum. In: IEEE Transactions on Information Forensics and Security (2020)
35. Kollreider, K., et al.: Real-time Face Detection and Motion Analysis with Application in Liveness Assessment. IEEE TIFS (2007)
36. Sousedik, C., Busch, C.: Presentation attack detection methods for fingerprint recognition systems: a survey. In: Journal on Biometrics. IET (2014)
37. Raghavendra, R., Busch, C.: Presentation attack detection methods for face recognition system - a comprehensive survey. In: ACM Computing Surveys (2017)
38. Steiner, H., Kolb, A., Jung, N.: Reliable face anti-spoofing using multispectral SWIR imaging. In: IEEE Proceedings IEEE/IAPR International Conference on Biometrics (2016)
39. Venkatesh, S., et al.: Face Morphing Attack Generation & Detection: A Comprehensive Survey". IEEE TTS (2021)
40. U.S. NIST Face Recognition Vendor Test: Part 4: MORPH - Performance of Automated Face Morph Detection. NISTIR 8292 (2022)
41. Kolberg, J., et al.: Template protection based on homomorphic encryption: computational efficient application to iris-biometric verification and identification. In: Proceedings of IEEE International Workshop on Information Forensics and Security 2019 (WIFS 2019), Delft, NL, December 9-12 (2019)
42. Boddeti, V.: Secure face matching using fully homomorphic encryption. In: Proceedings BTAS (2018)
43. Drozdowski, P., Rathgeb, C., Busch, C.: Computational workload in biometric identification systems: an overview. In: IET Biometrics (2019)
44. International Civil Aviation Organization: ICAO TRIP Guide on Evidence of Identity (ICAO TRIP) Strategy (2018). https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidtnqh_9;ence%20of%20Identity.pdf
45. Buchmann, N., et al.: A preliminary study on the feasibility of storing fingerprint and Iris image data in 2D-barcodes. In: Proceedings of the IEEE 15th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 21-23 (2016)
46. U Project: Fast and Trustworthy Identity Delivery and Check with ePassports Leveraging Traveler Privacy (2016)
47. CEN/TS 17489-1:2020: Personal Identification - Secure and Interoperable European Breeder Documents - Part 1: Framework Overview

(2020). https://standards.iteh.ai/catalog/standards/cen/6282fb8b-b57b-49ff-87f7-7f4c2686f8cd/cen-ts-17489-1-2020
48. Elfors, S., Zwattendorfer, B.: Using FIDO with EIDAS Services: Deploying FIDO2 for EIDAS QTSPs and EID Schemes. FIDO Alliance (2020)
49. Raja, K., Raghavendra, R., Busch, C.: Multi-modal authentication system for smartphones. In: Proceedings of the 8th IAPR International Conference on Biometrics (ICB), 19-22 May 2015, Phuket, Thailand (2015)
50. Nautsch, A.: Preserving privacy in speaker and speech characterisation. In: Science Direct, Computer Speech and Language Journal (2019)
51. Nickel, C., Brandt, H., Busch, C.: Benchmarking the performance of SVMs and HMMs for accelerometer-based biometric gait recognition. In: Proceedings of the IEEE Symposium on Signal Processing and Information Technology (ISSPIT), December 14-17 (2011)
52. Martinez-Diaz, M.: Graphical Password-Based User Authentication with Free-form Doodles. EAB award (2014)
53. Blasoc, J., et al.: A Survey of Wearable Biometric Recognition Systems. ACM Computing Survey (2017)
54. Liu, S., et al.: Recent Advances in Biometrics-Based User Authentication for Wearable Devices: A Contemporary Survey. ScienceDirect, Elsevier (2022)
55. Migo-Boras, A.: Fact Sheet (2010). https://www.marechausseecontact.nl/pdf/factsheet-migo-boras.pdf
56. Dekkers, T.: Mobility, Control and Technology in Border Areas: Discretion and Decision-Making in the Information Age. PhD thesis. Universiteit Leiden (2019)
57. Faraj, M., Bigun, J.: Synergy of lip-motion and acoustic features in biometric speech and speaker recognition. In: IEEE Transactions on Computers (2007)
58. Busch, C., et al.: Verfahren und Vorrichtung zur Verifikation autorisierter Personen zur Steuerung eines Verkehrsmittels (2001). Patent application DE000010156737
59. Bergh Johnsson, D., Deogun, D., Sawano, D.: Secure by Design. Manning Pubns (2019)
60. Chattopadhyay, A., et al.: Towards a biometric authentication-based hybrid trust-computing approach for verification of provider profiles in online healthcare information. In: IEEE Security and Privacy Workshops (SPW) (2017)
61. ISO/IECDirectives: Part 1 Procedure for the Technical Work (2022)
62. European Commission: Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonsied Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (2021)

How to cite this article: Busch, C., et al.: Facilitating free travel in the Schengen area—A position paper by the European Association for Biometrics. IET Biome. 12(2), 112–128 (2023). https://doi.org/10.1049/bme2.12107