SECURE IDENTITY ALLIANCE

Biometrics in identity:
Building safe and inclusive futures and protecting civil liberties

A good practice guide

2022 Edition

Mentions

Secure Identity Alliance (SIA)

Secure Identity Alliance (SIA) is a global non-profit association representing actors and organizations and adjacent industries active across the digital identity ecosystem. SIA's mission is to unify the ecosystem of identity and unlock the full power of identity so that people, economy, and society thrive. The association supports the development of the activities of its members across four broad pillars: Identity for Good, Outreach, Open Standards Development and Industry Services and Solutions.

www.secureidentityalliance.org

Design

Design Motive Ltd

Photo credits

iStock / Shutterstock

Editorial review

Slingshot Communications

We would like to thank the many contributors to this paper. Without their valued inputs, it would not have been possible to create such a detailed analysis of today's secure documents, the threats they face, and the security features in place to mitigate risk.

Production

This report has been produced by the **SIA Borders & Biometrics Working Group,** comprising:

Michael Brandau, Veridos
Chair of the Working Group

Frank Smith
SIA Advisory Observer, and lead author

Nicolas Phan
Emmanuel Wang
Idemia

Pascal Janer
Nicola Leotta
Vincent Roux
IN Groupe

Francoise Bergasse
Roger Edwards
Thales

Perrine Catinaud
Christina Schäffler
Jörg Senekowitsch
Veridos

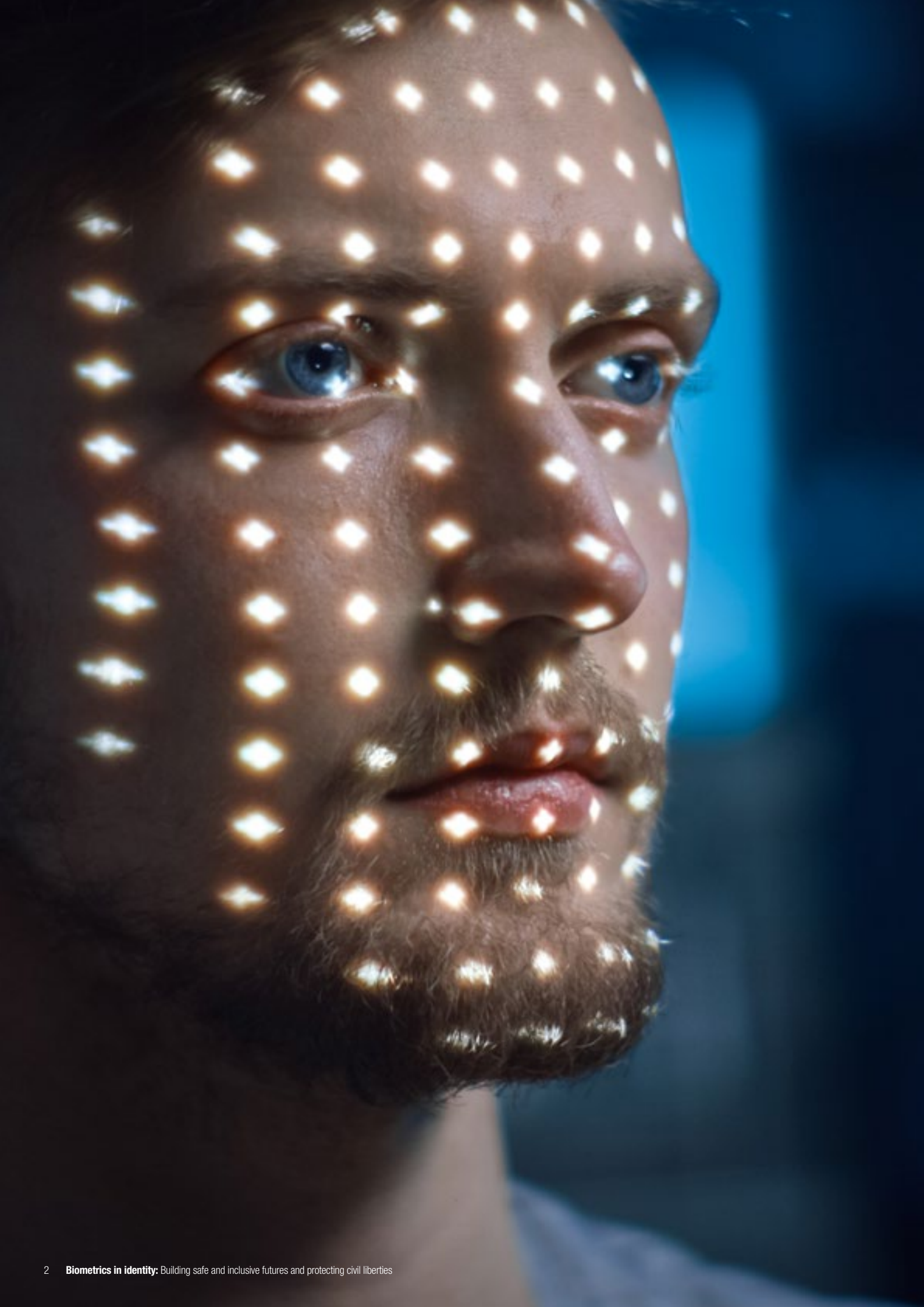
Patrick Lunven
Entrust

Thank you

Many thanks for the contribution of colleagues in the SIA Borders & Biometrics Working Group, also the SIA Secure Documents Working Group (Chair, Joachim Caillosse, IN Groupe) and other colleagues for their contributions.

SECURE IDENTITY ALLIANCE

Contents



1.
Executive summary

This report by the Secure Identity Alliance (SIA) seeks to support those planning and implementing biometrically-enhanced identity programmes and associated services.

Taking a holistic view of today's sophisticated biometric landscape, the report sets out the imperative for identity meeting economic, social and security requirements; explains how this is supported by biometric computer systems; highlights key issues that such systems need to consider; and offers a good practice toolkit. There is also a range of case studies presenting examples of current systems.

The review of biometric systems covers how the technology has evolved, the benefits to be gained from the use of biometrics, modalities (such as face, fingerprints and iris) and their selection, hardware, sensors, presentation attack detection, and the role of artificial intelligence and machine learning.

Examples discussed include major national and regional identity systems and several specific examples for border control, airport security, policing and asylum support.

This report emphasises the critical importance of stakeholders deciding what a new system must do. There are no universal or simple answers: the right biometric system should meet the required use case(s) and deliver the desired outcome within the societal, ethical, operational, security and budgetary context.

2. The identity imperative

2.1
The critical role of identity

A legally recognised Identity is one of the most important human rights in the modern world – as enshrined in article 16.9 in the **UN Sustainable Development Goals:** "to provide legal identity for all, including birth registration" by the year 2030. It was also the impetus for the launch in 2017 - by a group of 25 development partners, United Nations and international organisations, government agencies, foundations, civil society, and private sector associations including the SIA - of the **Principles on Identification for Sustainable Development** initiative **[REF-1]**. Revised in 2021, the objective of these principles is to serve as a "north star" for action and implementation in support of evolving ID systems that fulfil the promise of inclusive, sustainable development while mitigating the risks.

Around the globe, citizens depend on government issued identity credentials to prove they are who they say they are, and to undertake commonplace transactions like opening a bank account, registering for school, obtaining formal employment, or receiving social welfare transactions.

Identity is a validation of who we are. While we only need to expose just enough to enable secure and trusted authentication, there is little doubt that ID is becoming increasingly essential for full participation in our daily social, working and political lives.

This is the case whether we're streamlining citizen access to digital government services or delivering unique, personalised digital identities that make it easy for companies to know and serve customers better. It is nothing short of a strategic necessity for governments and commercial organisations everywhere.

Ultimately, citizens throughout the world depend on government-issued identities, evidenced by trusted identity credentials, to access a host of health and welfare programs, education, financial services, and to move smoothly and securely across borders.

Identity management systems are central to effectively addressing population movements and the continuing challenge of refugees in the world, as well as facilitating national security and anti-terrorism activities, while being a catalyst for sustainable economic growth and inclusion.

2.2
The need for legal, trusted identity

In response to growing citizen demand, governments around the world are fast tracking the shift to digital service provision. But, with multiple identity providers offering to host and manage digital identities for the general public, the **root identity – the single sovereign trusted identity upon which all others are based – must start with government.**

Principles on identification for sustainable development [REF-1] www.idprinciples.org

INCLUSION: **Universal Coverage and Accessibility**	**1.** Ensure universal access for individuals, free from discrimination. **2.** Remove barriers to access and use.
DESIGN: **Robust, Secure, Responsive and Sustainable**	**3.** Establish a trusted – unique, secure, and accurate – identity. **4.** Create a responsive and interoperable platform. **5.** Use open standards and prevent vendor and technology lock-in. **6.** Protect privacy and agency through system design. **7.** Plan for financial and operational sustainability.
GOVERNANCE: **Building Trust by Protecting Privacy and User Rights**	**8.** Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework. **9.** Establish clear institutional mandates and accountability. **10.** Enforce legal and trust frameworks through independent oversight and adjudication of grievances.

Trust is critical in the digital ecosystem. As custodians of the 'root' identity, governments need to build their digital identity strategies in a manner that ensures they can retain control of national services and transactions, protect their citizens and allow individuals to use their derived digital identities as access points to commercial services – without exposing it to theft, misuse or attack.

This is particularly true when it comes to the collection, management and use of biometric data. Government, border management and law enforcement use cases typically require the development of biometrically-enabled identity. As such, there is a strong argument that the state possess a considerably more legitimate reason to create and maintain biometric databases than private enterprises.

At the most fundamental level, the effective development of a **secure and trusted identity** relies on **two pillars** – all of which increasingly utilise the individual's biometrics:

- The creation of the **root identity** within a well-functioning civil registration and vital statistics system based on a unique set of characteristics (biometric and/or biographical data).
- The creation of secure, **government-issued credentials** (physical or digital), such as a certificate or passport, by which the individual can seek to prove their identity.

There's more to it, of course. Such as ensuring that a biometric record taken at a particular point in time is tied to the root identity – for example when applying for a new passport, during an interaction with law enforcement, or adding biometrics to authenticate access to a state-run welfare program. Here, the ability to tie back to the root identity is critical for ensuring both accuracy and security and requires a clear set of processes whatever the application.

Whether embarking on a government-driven centralised system in which state-issued digital ID serves as the basis for all public and private sector transactions, initiating a federated model of multiple government-endorsed digital identity providers, or supporting a decentralised approach, the definition of what constitutes official legal identity should always remain the purview of the state.

Across the world, policy makers are required to navigate all these complex issues. The scale and sophistication of today's identity systems, the complex integrations, and the broad and interconnected ecosystems of multiple public and private stakeholders combine to pose considerable challenges. As do the potential tensions between national security and individual privacy.

For many the role of biometrics in addressing these issues and in protecting user identity, guaranteeing goods and services make their way only to bona fide recipients, and reducing fraud and abuse, is without equal.

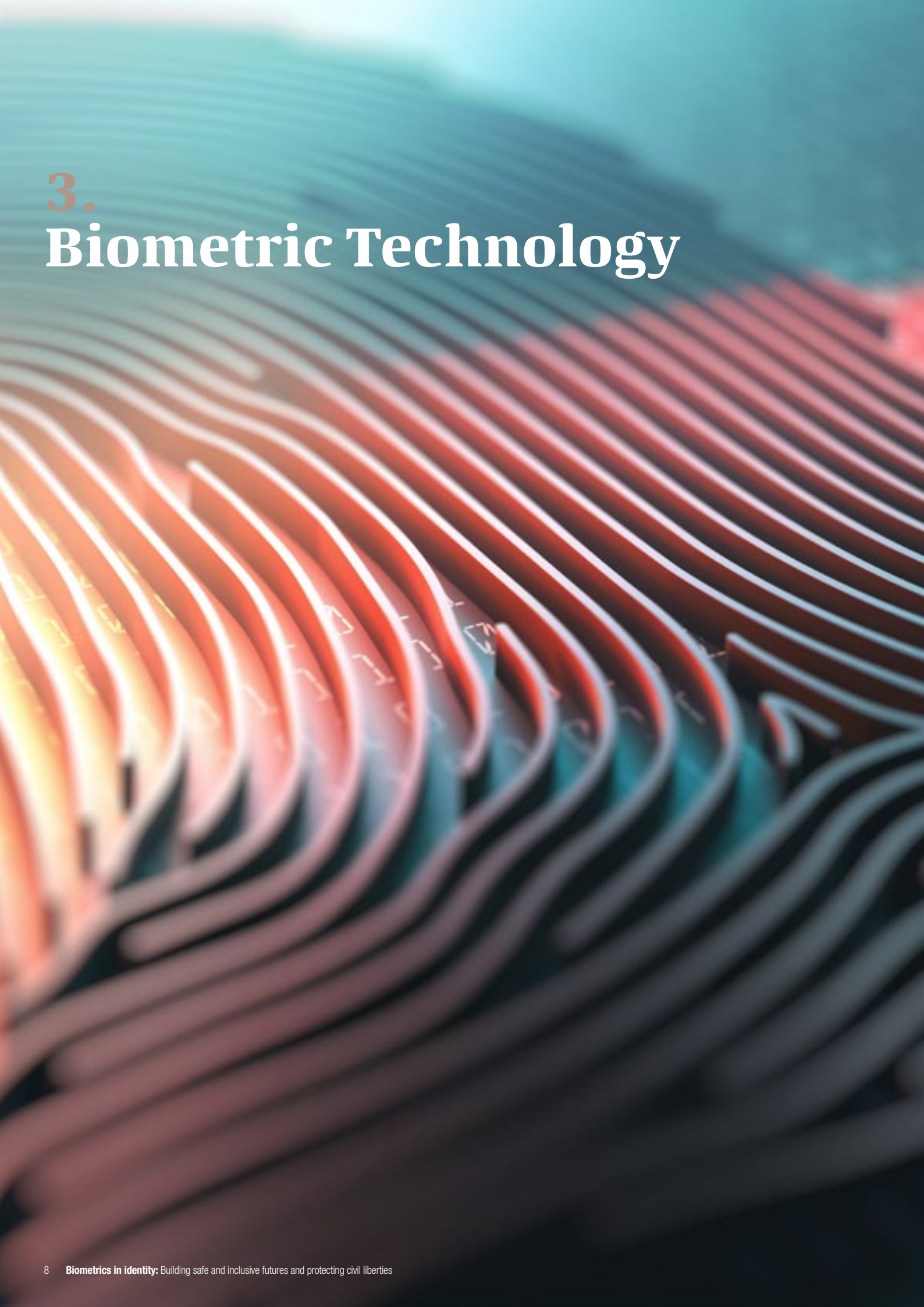
Only by knowing 'who' to a high degree of certainty can government or business ensure that only those entitled are being served. To do otherwise is both an economic and social injustice and biometrics technology has now advanced to a level where performance is proven, and the benefits are real and measurable, and easily outweigh the costs.

Only by knowing 'who' to a high degree of certainty can governments or business ensure that only those entitled are being served.

The quality (accuracy, timeliness, completeness, etc.) of data and the correct operation of each system is also essential. Data inherited from legacy systems that does not already meet a rigorous standard may be hard to correct after the event: an approach to linking identity (as described above) may be easier to implement for new data than to cleanse historical data.

As an example, the EU has strengthened the security of European ID Cards and Residence Documents, bringing these into line with the existing security standards for European Passports and Residence Permits aligned to ICAO 9303 plus the European requirements for including fingerprint images (Extended Access Control (EAC)). This is contained in EU Regulation 2019/1157, which came into force 2 August 2021 and is seen as an important contribution to European efforts to control immigration and counter terrorism.

3. Biometric Technology



3.1
How biometric technology has evolved

Origins

Fingerprints as a means of identification in criminal cases and police investigations began around the start of the 20th century, but processing collections of fingerprints was time-consuming and manually-based. This in turn limited the accuracy and the size of collections that could be searched in practice.

The modern era of fingerprint systems began with the development of Automated Fingerprint Identification Systems (AFIS) around the 1970s and 1980s. Since these early systems first appeared, the capability of AFIS and Automated Biometric Identification Systems (ABIS) have improved radically. As a result, the size of biometric databases, the performance and speed of processing, the number of simultaneous users and range of applications has similarly been transformed. Biometrics is no longer confined to the criminal context but is also an important means of allowing citizens to have their identity recognised by the state which, in turn, enables benefits to flow from that recognition.

We look at some current examples of biometric ID in the following section.

National core biometric systems

At the top end of the scale, the case studies in this report include several major examples of national core biometric systems. **Aadhaar** now holds biometric details of over 1.25 billion citizens in India; and the case studies include **Burkina Faso's** voter registration system, one of an increasing number being built. Law enforcement systems across the **EU member states,** and in the **USA** and **UK** support rapid access by police and border authorities and help to safeguard the public against criminal activities. Adding such large, biometric-based systems to systems that have previously not had biometric capability is complex, requiring extensive integration, of technology, infrastructure, operations (to high levels of reliability and security) and effective leadership and co-operation between multiple partners to deliver these challenging projects.

Systems with more specific functionality

Since automated **e-Gates** using facial recognition began to appear at airports from 2010 onwards to allow lower-risk travellers to enter the country, the use of this technology has matured and expanded considerably as border control services have gained confidence in its use. More recently, similar facial recognition has been used to improve the efficient flow of travellers through airport security and boarding, avoiding repeated inspection of identity documents after the person enrols once on entering the airport. Often referred to as **frictionless travel,** facial recognition is increasingly being used across the world and this report contains a number of case study examples including Spain, France and Columbia. See also the NIST report on facial recognition and paperless travel [REF-2] and the eu-LISA Industry Roundtable report on paperless travel [REF-3].

The Eurostar case study takes this use case further, allowing selected passengers travelling by train from the UK to France to enrol their travel document and facial photo from home, using their mobile phone, in advance of arriving at the station for departure. EU countries are also equipping ports with the capability to enrol and verify passengers' biometrics so that they can operate the new Entry Exit System (EES) – see the France case study for more detail. In some cases this task is being done using mobile technology.

Queuing for border control and security can be a frustration while travelling, but these controls are important to deliver security to protect against terrorism, organised crime and immigration abuse. Furthermore, the smart use of biometrics can increase security and make the experience quicker and simpler for travellers.

Commercial systems

Biometric systems are also playing an growing role in the commercial arena including onboarding new accounts, securing online transactions, providing access to bank and other digital services, and ATM cash withdrawals. Over 20 biometric payment card pilots are currently active globally and the first commercial deployment by BNP Paribas has been launched. It will not be long before consumers everywhere will be able to embrace on-card biometric fingerprint authentication for everyday payments. See paper by the Smart Payment Association [REF-4]. Some bank call centres now use voice biometrics to authenticate callers.

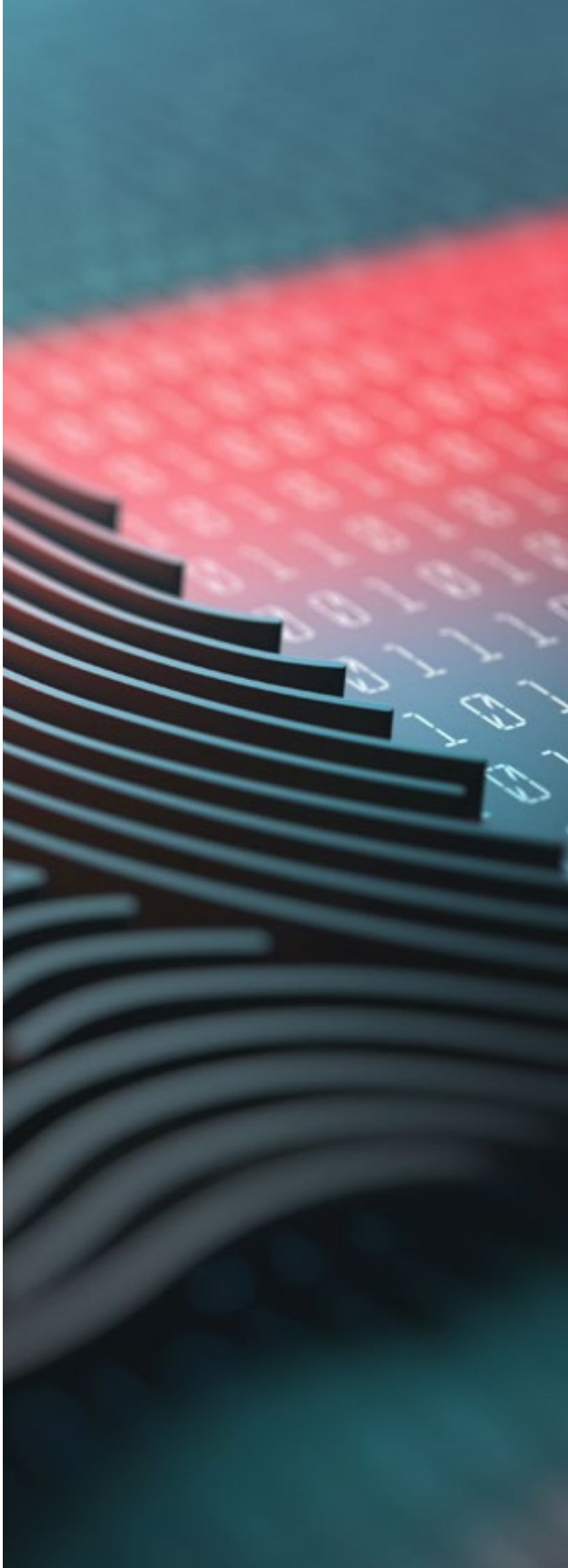
Mobile systems

The widespread use of mobile phones and their inclusion of fingerprint and face biometrics has been significant in the last few years. These enable mobile phones to be used with NFC communications for cashless payments, linked to the user's bank account. The biometric capability of mobile phones is also being used in connection with applications to official systems – cases include visa and residence applications, passing through security checks at airports and the border, opening back accounts and giving identity and age checks online and at retail points of sale. Fingerprint and face biometrics are widely used to simplify access to mobile phones.

Connected remotely to central system, smartphones can read travel documents for verification, test for liveness and attempts to use false biometrics (spoofs). Used by police and border services (in accordance with privacy legislation) mobile phones can be used to enrol biometrics and search central systems. In Finland mobile border control will be undertaken when EES is in force, enrolling and verifying biometrics on trains entering the EU.

The future?

There have been many important developments in this field and further development and innovation will surely continue for some time to come.



3.2
Benefits from the use of biometrics

The following illustrate the key benefits of using biometrics within both identity and authentication contexts:

To prove Identity

The use of a secure, accurate biometric, rigorously verified against the holder of a passport or ID card can add important assurance on identity, in addition to any checks on the authenticity of the document itself. Biometrics, therefore, play an important role in preventing identity theft or fraud.

To enhance security

Biometric authentication offers a higher level of security than other methods of online identification. Between social media accounts, emails, application and services, the average person might have upwards of 20 different identities. Trying to keep track of our various logins, passwords and PINs is an almost impossible task – forcing people to use the same password/PIN for multiple uses which makes them vulnerable to hacks. Biometrics makes having to memorise multiple passwords a thing of the past.

To improve customer experience

Consumers/citizens want an improved experience. We all want user-friendly and highly secure ways to undertake our daily life tasks, but traditional forms of authentication can feel clunky and inconvenient. Biometrics can go a long way to eliminating the complexity and time involved in securely boarding an aeroplane or cruise ship, moving between borders, paying for products and services and more.

To enable financial inclusion

Supporting the next wave of financial inclusion. Globally, many adults remain unbanked – without an account at a financial institution or through a mobile money provider. Often this is as a result of the lack of appropriate documentation to prove their identity. Biometrics offers significant potential to address unbanked populations and case study on the Indian government's Aadhaar system is a good example of this in practice.

To manage migration & population movements

Biometrics offers a truly transformational opportunity to address today's growing migration challenges. Not simply to monitor population movements for border control and security purposes, but to provide previously undocumented migrants with an identity to access support services for humanitarian aid, for example in war or disaster situations.

3.3
Biometric modalities

While there many potential types of characteristic that can be used for biometric capture, matching and searching, the most common characteristics (or modalities) in use today are detailed below. These are selected to provide uniqueness, permanence, and consistency – providing accurate recognition and a high level of protection against fraud, while also being conducive to being captured using sensing devices in an ergonomic, non-invasive and convenient way.

Facial recognition

One of the most flexible biometric identification methods, facial recognition systems analyse features common to every individual's face: the distance between the eyes, the position of cheekbones, jaw line, chin, width of nose, shape of mouth and so forth. Systems can automatically identify or verify an individual from a digital image or video frame, comparing selected facial features from the chip-stored image of an electronic travel document or a facial database. Facial recognition is widely used for identity verification and identification in many border control systems including the EU, USA, APAC, followed by South America, and more recently by the Middle-East where systems are using facial biometrics as a primary modality to process border movements.

Fingerprint recognition

While there is some evidence that fingerprints degrade slightly with age, finger ridge configurations remain unchanged throughout the life of an individual and therefore are a good indicator of identity. Fingerprint patterns too are another accurate and reliable identifier characteristic – and this approach is gaining widespread popularity for personal identification systems owing to its distinctiveness and stability. Recent advancements in technology have led to the development of fingerprint recognition systems that are small and inexpensive – resulting in the deployment of these systems in a wide range of scenarios. Applications include mobile phones and laptops; access control to buildings; and law enforcement including policing and border control – but requirements vary considerably.

Iris recognition

An authentication method that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eye, using near infrared (NIR) light—normally requiring NIR illumination. The iris of the eye has a distinct pattern that remains stable throughout a person's life. These highly accurate biometric systems are rarely impeded by the presence of glasses or contact lenses and are well suited to one-to-many identifications. Iris recognition systems have been implemented in Aadhaar; UAE airports and land and sea ports; the FBI has incorporated the technology into its next-generation biometric identification system; and Google uses this iris recognition to regulate access to its datacentres.

Other modalities

Other characteristics may also be used to identify a person such as palm, voice, finger vein, gait. DNA has been a vital source of forensic evidence particularly in criminal cases. Dental records are often used to confirm the identity of a deceased person, especially when soft tissue has deteriorated.

3.4
Selecting the right biometric modalities

The selection of the modality is largely dependent on the use case. Systems can also be designed to use a single biometric identifier for identification or verification. These are called single or **unimodal** systems. It is becoming increasingly common to see two or more biometric modalities used together, in **multimodal** systems.

There are pros and cons for both approaches. Unimodal systems benefit from being simpler and generally less expensive in terms of enrolment, required hardware and software, and data management. There are also cultural and ethical considerations – different populations and cultures may be happier to register one or more biometric modalities to avoid multiple identity checks when calling their bank, for example. But they may not want to register a different biometric modality – the choice may differ from one country or region to another.

Reassurance about safeguarding the personal privacy of data collected may also influence public acceptability. A solution that stores a person's biometric information on their smartphone without sharing it may also help user acceptability and can simplify privacy implications for the service provider.

While multimodal approaches require users to register more of their unique physiological data, they also provide a higher level of assurance that the individual is who they say they are. This can reduce the number of false negatives/positives and increase the reliability of the recognition – addressing the issues caused by aging irises in older people and in fingerprint scanning systems for younger children whose ridges may not be fully developed.

The multimodal approach has also been shown more effective to address vulnerabilities posed by spoofing biometrics and sets a higher authentication threshold that increases security – making them more appropriate for national eID schemes, ePassports and voter registration programmes.

Adding another modality will increase cost but does not automatically increase the effectiveness of a biometric search (1:Many) or verification (1:1 comparison). Other factors impact accuracy including the quality of the biometric sensor, resolution of the image, the sophistication of the enrolment and matching algorithms, and level of presentation attack detection (see below).

The right choice is the one that best meets the requirements, with the 'right' **balance** between security, convenience, cost and other factors that must be considered before an informed decision is made **for the particular circumstances.** Requirements may vary widely between different systems and use cases.

3.5
Sensors

Sensors are an important component in a biometric system. They vary considerably in type, capability, size, weight. They need to be **right** for the intended purpose, not necessarily the **best** possible for the task. Over-specifying sensors may for example result in excess cost and use of data storage (for larger images) and may not give the most usable result.

A fingerprint sensor may capture **flat** or **rolled** fingers; differ considerably in size of sensor platform and biometric accuracy. If flat, individual fingerprints are not required (see below), a 4-finger 'slap' reader can capture 4 fingers in a single image and can capture 10 fingers in 3 or 4 such slaps (4 fingers twice, plus 2 thumbs captured together or separately). Some devices use lightweight thin-film sensors which are more portable; others are heavier desk-based devices. Some require the fingers to make physical contact with the surface of the sensor; others are contactless. Some systems for mobile smartphones allow capture of fingerprint images as for a slap, via the on-board camera.

None of these is universally the right one to select: it is important that the requirements are properly understood and matched with the most appropriate solution. A balance may be chosen between the extent of the image(s) recorded, and convenience and speed of capture. As an example, the identification standard for EU's EES is one 4-finger slap, plus a facial image [REF-5].

3.6
Fingerprint image quality

The quality of fingerprint images is critical to the correct functioning of an AFIS system: poor quality images will lead to incorrect identification results. Where accuracy is essential, for example in many criminal cases, an identification may be reviewed by a qualified fingerprint expert before being confirmed. Some relevant metrics are:

- **False Accept Rate (FAR)** and **False Reject Rate (FRR)** measure respectively the percentage of incorrect **matches** made (not being the same person); and the percentage of incorrect **non-matches** made (when they are the same person)
- **NFIQ 2** is a quality assessment tool from the US National Institute of Standards and Technology (NIST), using open source software. This links image quality of optical and ink fingerprint images at 500 pixel per inch to operational recognition performance [REF-6]. NIST also defines a **file format** for transporting fingerprint images
- **Fingerprint Acquisition Profile (FAP)** is a number representing the capability of optical devices used for fingerprint capture, e.g. FAP 10, FAP 30, FAP 45, FAP 60 or higher

The most significant exception to high quality images is in the case of fingerprint images left at the scene of a crime, known as **latent fingerprints.** These may need special processing to make them visible, and may be degraded (e.g. smudged, incomplete, not covering the centre of the print and/or ambiguous as to which finger has made a print). The requirement to be able to identify someone from such prints increases the need for fingerprints enrolled normally onto an AFIS system to be of consistently high quality and may require prints to be captured as rolled rather than slap images, to increase the area of fingers recorded.

3.7
Presentation attacks and detection

Various attempts may be made to deceive biometric systems by presenting a false biometric sample (a presentation attack). Examples can include:

- Morphed photographs – combining features of two or more people, typically when a photo is submitted as part of a passport application. The resulting passport may be accepted a human observer or a biometric computer system when presented by any of the people whose photo is merged into the false facial image
- Deep fake videos – advanced software may be used to take a static photo of someone and manipulate the face to make it appear to 'speak' words spoken on a soundtrack: this may produce a video that appears realistically to show the person speaking words they have never in fact said
- False biometric samples – someone can try to disguise their appearance for example with false or altered facial hair, a wig, a mask, distracting jewellery or coloured contact lenses; or false latex covers (gummies) on their fingertips to present an altered fingerprint pattern

Responses are known generally as Presentation Attack Detection (PAD). This can include a highly accurate comparison of facial images to detect the differences between a real subject and a morphed image, and real-time liveness detection online. There is a role too for human operators in paying close attention to the subject's face and fingers when a person is being scanned with a biometric reader. The ISO/IEC 30107 standards give a basis for devising and testing PAD capability: testing and certification services are available. Artificial intelligence (AI), below, is also an important contributor.

3.8
High performance hardware

Large fingerprint and other biometric systems require high computing performance. Although processing continues to get more powerful (known as Moore's Law), the demands also increase as the number of biometric modalities, complexity of encoding schemes and matching algorithms, database size, number of simultaneous users, enrolments, and demand for real-time access and search results all increase. Traditionally these systems have included multiple specialised computers called matchers for biometric searching, often hosted in an in-house data centre. This approach is still extensively used. However, where the customer sees sufficient advantages in price, flexibility and reduced complexity, cloud solutions hosted outside the organisation may sometimes be used – provided the organisation is satisfied on privacy and security, considering where the cloud storage is held and who has access and control. A private cloud can give advantages of cloud organisation, held entirely within a large organisation. The balance may perhaps shift towards more cloud solutions in the future.

3.9
Artificial intelligence (AI) and machine learning (ML)

AI and ML have wide application and are delivering important advances in the effectiveness of biometric systems and the broader infrastructures they form part of.

The report of an industry round table by the eu-LISA agency, **Artificial Intelligence and Large-Scale IT Systems, November 2021** [REF-7] contains an examination of AI in biometric recognition technologies (Session IV in the report). A range of industry, government and academic speakers participated: key points included:

- AI has a significant role for example in big data analysis and decision-making in large identity-based systems where biometrics may be an important component.
- A cross-European research project on how biometric technologies can improve the automation of border crossing identified the need for seamless connection; compliance with legislation (EU values and regulations) and pandemic-related restrictions; and low vulnerability to adversary attacks. (Dr Luigi Rappaele, Frontex).
- AI, or more particularly deep machine learning (ML), has made a significant improvement to facial recognition reducing false negative identification rate from just under 4% to 0.16% between 2018 and 2021 according to Industry Experts. (Previously, Patrick Grother and colleagues at NIST reported in 2018 [REF-8] that although there were still wide variations, massive gains in accuracy had also been achieved by many face recognition algorithms from 2013 to 2018. The gains stemmed from the integration, or complete replacement, of prior approaches with those based on deep convolutional networks. As such, the authors concluded, face recognition had undergone an industrial revolution, with algorithms now more tolerant of poor-quality images.
- With good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with error rates below 0.2%. However, when significant age differences existed, or the photographs were of lower quality, some struggled.
- Improvements have been made in detecting presentation attacks, but this is better where known sensors / readers are used under fully controlled circumstances. The task is harder where unknown sensors are used in uncontrolled circumstances.
- Morph Attack Detection (MAD), a more specific instance of PAD, has benefited from analysis of common tools used by criminals for morph production, a number of which are open source. One European country has detected 40 morphed images, all related to organised crime.
- PAD improvements are also being sought through video analytics, to test the validity of video streams.

A top concern revolves around questions of ethics and equity, specifically concerns of bias, where opponents say technology may not be as reliable depending on a person's gender or ethnicity and misidentification (False Match) and their potential unqualified consequences. Many of these claims are based on the performance and results of older tests that used limited and unrepresentative datasets. However, the performance of the algorithms is a direct correlation to the data included in the database [REF-9].

4.
Biometric Governance

As stated earlier, building a cohesive and interconnected biometric ID infrastructure and associated services is complex. There are a multitude of considerations to be assessed, from the ethical and legal, to the technical and operational. Furthermore, it requires the buy-in and collaboration between multiple stakeholders, and involves several obligations and expectations on those setting up and operating biometric systems. In this section we look at the key considerations of any biometrically-enhanced identity service regarding privacy, security, inclusion, the use of artificial intelligence, standardisation and data sharing.

4.1
Privacy

As previously discussed, privacy is the number one concern for citizens. This is perhaps best illustrated by the growing deployment of facial recognition systems in tandem with behavioural biometrics and AI. Whether in a retail scenario to identify shoppers or a national security use case, it will be important to plan and deploy AI-powered biometric systems ethically and responsibility – with the rights of the individual uppermost in the minds of policy makers.

General Data Protection Regulation (GDPR)

In Europe, and for European-operating organisations, the General Data Protection Regulation (GDPR) offers some regulatory cover in terms of an individual's privacy. Here, biometric data is specifically identified as a 'sensitive category of personal data', with biometric data being defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data". Certain GDPR exemptions exist for personal or household activities, law enforcement and national security.

Under the terms of the regulation, there are now well-established norms for capturing, storing and processing personal data, with stringent opt-in conditions. Similarly, the eIDAS (Electronic Identification, Authentication and Trust Services) set of standards for electronic transactions in the European Single Market lay down some protections in Europe (and for European citizens).

In the EU two fingerprint images are now included in Schengen area passports and ID and other residence cards but access to this private information is strictly limited, using Extended Access Control (EAC), under EU Regulation 1157/2019.

Privacy-by-Design

Privacy-by-Design matters, whether in a national identity scheme, a border security environment or in a consumer-to-brand relationship. The Privacy-by-Design principles and framework were established by Dr Ann Cavoukian from the University of Ryerson in Toronto (CA) in the 1990s and is an inspiring source of best practices internationally [REF-10]. The right of the individual to privacy must be properly protected. Indeed, individuals who increasingly consent to their biometric data being stored and processed must be able to do so with a high level of confidence that their data is being used for the specific purpose it was provided for – and no more. This is as relevant an issue for government agencies sharing biometric information with one another as it is for commercial organisations wishing to deepen their customer profiling activity.

The 7 foundation principles of Privacy-by-Design are:

1. Proactive not reactive; preventive not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

As with many such evolutions, the pace of technology change within biometrics is outpacing many regulators' abilities to provide appropriate control mechanisms. This is particularly true with IoT-enabled biometric data capture and processing. How international and national regulatory authorities continue to address the privacy issue must remain in focus as we move forward.

To date there is no universal international standard for biometric data protection. There is, however, a tranche of technical standards relating to interoperability that we cover below in the section on data sharing.

Privacy matters, whether in a national identity scheme, a border security environment or in a consumer-to-brand relationship.

4.2
Security

Privacy and facial recognition

Facial recognition has advanced considerably in its capability in recent years, and with a good camera and lens it can be used at a distance without someone passing within range being aware that they are being identified and checked or recorded on a database. This can raise controversial public debate on privacy and as a result some local jurisdictions have banned use of facial recognition. However, facial recognition has some clear benefits that are widely supported, including convenience and protection against terrorists and serious criminals.

In 2018 [REF-11], Microsoft President Brad Smith lobbied for a wider discussion of facial recognition technologies, calling on governments around the world to adopt laws to regulate this technology. He proposed the adoption of 6 principles — fairness, transparency, accountability, non-discrimination, notice and consent — and for surveillance by law enforcement to be conducted within a legal framework.

In 2021 the Council of Europe set out guidelines on the use of facial recognition [REF-12] with specific considerations for legislators and decision-makers; developers, manufacturers and service providers; and entities using facial recognition technology. Consideration was also given to the rights of data subjects.

The SIA view is that a sweeping ban on facial recognition would be premature. Whilst facial recognition can be used in a way that would raise concerns about mass surveillance, data protection and cybersecurity risks, it can produce real benefits, as demonstrated in enabling citizens to enrol and verify their identity remotely during the COVID-19 pandemic. But it is vital that industry and regulators work closely together to address the very real concerns this technology can pose. See SIA Blog on facial recognition [REF-13].

The security of biometric data is, of course, paramount. A biometric system is inherently one that stores personal data, which therefore requires high levels of protection against attack and from improper processing (such as disclosure to anyone not entitled to receive it). The spectre of a widespread data breach of the biometric data of millions of citizens is of major concern.

While at rest, biometric data collected (and the associated templates generated) from biometric capture devices should be stored in a secure, dedicated environment to avoid theft or leakage that would expose the data to malicious usage. This is particularly relevant for networked capture devices such as cameras.

Encryption is required – whether data is stored on the device, or in the case of centralised databases on-premises, in a virtual, public cloud, or hybrid environment. In transit too, biometric data should be encrypted and sent across secure channels to prevent theft as data travels between the device and the database where it is stored. On mobile devices sensitive data can be secured via Trusted Execution Environments (TEE) or Secure Element.

Similarly, secure access management and user management are crucial to restrict access only to entitled persons to systems and specific information. Provision should also be made to trace and store access data from authorised individuals, as well as unauthorised access attempts.

Additional security can be added with two-factor authentication to support the digital ID, through passports or identity cards. While the direction of travel is certainly digital-first, physical identity documents will continue to play a key role for years to come. Indeed, the Aadhaar initiative utilises a 12-digit code for authentication – adding the something I have to the something I am. This ability to interact with digital documentation in areas of limited connectivity is crucial in many parts of the world today.

Protection of online access can be strengthened by liveness detection to address spoofing attacks. Improving sensor technology and matching algorithms helps to counter such attacks. – see the earlier section on presentation attacks and detection.

We also see a tremendous amount of work to secure against, and open up new, biometric vulnerabilities. Photo-morphing is one example that has been shown to create highly plausible passport photographs – using increasingly advanced algorithms.

While no security solution is 100% effective – due in large part to the need to balance security with user convenience – it is also true that exposed vulnerabilities often result from the incomplete or incorrect implementation of technology (rather than the technology itself).

Exposed vulnerabilities often result from the incomplete or incorrect implementation of technology rather than the technology itself.

4.3 Inclusion

India has proved that, with enough determination, it is possible to implement a very large national identity scheme based on biometrics (see the Aadhaar case study). However, it is important that doing this improves inclusion particularly for citizens who are disadvantaged or hard to reach, rather than increasing their exclusion.

Under the model all ten finger images, a facial scan and an iris scan are collected. The case study illustrates how large an achievement this was, averaging 1/3 million enrolments per day for over a decade. To maximise inclusion, some 100,000 certified portable enrolment devices were deployed, bringing readily transportable equipment capable of operating in remote locations without electricity supply or online connectivity. This choice of bringing the enrolment to the citizen is a proven approach that drives higher engagement. This was a major but necessary exercise requiring a significant infrastructure investment, and a nationwide acceptance and enrolment process.

Effective inclusion means that those who are eligible to receive a benefit or entitlement from the state are able to do so, more easily and certainly; while others are more readily stopped from receiving these outcomes when they are not entitled, reducing fraud and strengthening good governance.

4.4
Artificial intelligence: legislation

In April 2021 the European Commission tabled proposals for a European regulatory framework for AI. This has been welcomed by eu-LISA in 2021 Industry Roundtable report mentioned earlier. For example, there may be concern that decisions previously made by real people, who can consider human factors and extenuating circumstances, a fully AI-based decision without reasoning ("the computer says NO!") might in practice be impossible to challenge. As with privacy, there is a view that a legislative framework is needed, but there is still a debate to be had on exactly what such legislation should say.

The European Union published proposals for legislation on Artificial Intelligence in April 2021 [REF-14], (these remain under consideration at the time of publication in 2022). The proposals recognise that AI is expected to bring a wide array of economic and societal benefits, but that concerns exist for example over fundamental rights and safety risks. The proposed legislation is intended to create the conditions for the development and use of trustworthy AI systems. Risks would be graded from unacceptable – to be prohibited; high – to be regulated accordingly; limited – which should be transparent; and low or minimal risk – which would not carry specific obligations.

The SIA recognises that biometrics and AI both have an important role to play in creating a legal, trusted identity for all, and in a blog article [REF-15] supports the creation of a fit-for-purpose framework, provided rules on the development and provision of AI systems are proportionate. However, it is concerned that some of the proposals under consideration could stifle innovation and therefore hold Europe back as a leader in this critical field and could conflict with data privacy or security needs. Some of the proposed principles may be hard to translate into concrete terms. The SIA notes it is also hard to define the rules for a technology that is still emerging.

4.5
Standardisation

The majority of technical deployments benefit from leveraging industry standards – and there are many relating to biometrics. These are complex and should be fully understood in the design of any biometric-based identity infrastructure and application to ensure the interoperability of both data and systems and to reduce development and lifetime cost. The interchangeability of components is vital too – both to simplify testing and to future proof systems.

However, in the biometric context, the sheer number of technical standards can create challenges. Indeed, both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) recommend against long reference lists of standards in this, and other, areas. When seeking to ensure standardisation, and corresponding interoperability of technology solutions, policy makers are advised to work with their industry partners from the beginning of the project to ensure standards compliance.

4.6
Data sharing

In a security and law enforcement context, data sharing is a well-established norm. A good example was the Migration 5 (formerly the Five Country Conference) High Value Data Sharing Protocol (HVDSP), established in 2009 to enable the exchange of biometric data between the immigration agencies of Australia, Canada, New Zealand, the UK and the US.

Latterly, the success of the HVDSP has encouraged members to develop a successor – the Secure Real-Time Platform (SRTP) - to enable high-volume automated exchanges. The objective is straightforward: to exchange data relevant to immigration cases while maintaining individual privacy, with 'privacy by design' as a cornerstone. With more biometric data becoming available, the sharing of such data is set to continue (see the case study on the UK Home Office Biometric Programme).

Moving beyond government, today's biometrically-enhanced authentication services do not, as a general rule, share biometric data. The biometrics held on today's crop of smartphones, and increasingly in biometrically-enabled smart payment cards is not shared. Rather the match is made on the device – where the biometric data is securely stored and encrypted. A simple yes/no verification message is transmitted to the Point of Sale terminal, not the individual's actual biometric information. Nevertheless, the potential to gather and share biometric information without the individual's knowledge creates an issue for both commercial and government policy makers, particularly as facial recognition and behavioural systems grow in importance.

5. Conclusions

… and a good practice toolkit

This report has presented a comprehensive tour of the issues relevant to the good and effective use of biometrics: the identity imperative, to which biometrics makes such a powerful contribution; the continuing evolution of biometrics; how biometrics can be used effectively and several of the components and decisions required to create such a system; governance, including the proper consideration of privacy. The annex to this report contains case studies of several solutions making notable use of biometrics, together with a glossary and references.

Ensuring the success of proportional, ethical and outcome-driven ID programmes is both an economic and social imperative. As the biometric-enabled identity market and its technology continues rapidly to evolve, it is more important than ever for regional and national governmental bodies and policy makers to make use of the expertise of today's wide and deep community of experienced best-of-breed partners.

The Secure Identity Alliance (www.secureidentityalliance.org) is an expert and globally recognised not-for-profit organisation. We bring together public, private and non-government organisations to foster international collaboration, help shape policy, provide technical guidance and share best practice in the implementation of identity programmes.

In conclusion, we present a good practice toolkit containing good practice ideas from the contributors to this report. There is no single 'right' way of building or operating a biometric system, but this toolkit is offered to those designing and running a system to help them consider important choices they need to make in order to build a biometric solution that meets their needs well.

Good practice toolkit

We hope that the ideas that follow are helpful in constructing your biometric system. Good luck!

5.1
Good practice toolkit

Understanding what you need, using the right expertise

Beware of developing or acquiring of a biometric system without fully understanding what you need, and make sure the solution delivers its objectives. Biometrics is not one size fits all solution. For a major system, relevant experts will need to be involved from the outset. Some requirements may be more complicated than a non-expert may expect and discussions that deliver deeper understanding on why certain advice is being recommended can be a useful learning process for the team, before a business decision is taken.

Security and privacy

A biometric system stores personal data, which therefore needs protection from attack and from improper processing, such as disclosure to anyone not entitled to receive it. Loss of personal data can be very damaging for the subject(s) and for the owner of the system and is subject to legislative protection – and potential penalties. Protecting data effectively not only relates to technical system security but to business processes and therefore staff training in the use of the data. Security is also important for protecting the correct functioning of the system, avoiding corruption or loss of data or processing capability of the system itself, for example in the event of cyber-attack. Additionally, user protections are critical, such as clear opt-in, opt-out options, the right to review data, and the right to delete data. While such protections are enshrined in Europe's GDPR, these are not yet universally available. However, for each implementation of a biometric solution it is highly recommended that a Privacy Impact Assessment (PIA) is conducted before implementation by an accredited agency or specialised law firm to guarantee that it is in full compliance with the GDPR relevant national legislation in the country of deployment.

Integration

A biometric system is not built for its own sake, but to create a biometric capability to support a broader business purpose. Therefore, effective integration, for example of planning, strategy, data, networks and user functionality, has to be envisaged from the start – and delivered. Look for partners with solid reputations, proven portfolios and a clear vision of the desired outcomes.

Proportionality

As we have seen in this paper, biometrics offers significant problem-solving potential – from secure borders through to social inclusion. But along with great power comes great responsibility. It's vital to remember biometric data are personal information and should be managed appropriately, proportionately and ethically. Using facial biometric capture to, for example, deter thieves from stealing toilet paper is arguably disproportional and raises ethical questions – particularly with regard to how that data is stored and processed. In Europe, the GDPR rules are quite clear, however similar regulatory oversight doesn't exist in all geographies around the globe. Just because governments can capture biometrics doesn't mean they should, and the use must be ethically as well as operationally appropriate under clear legitimate purposes.

Modality

As we have seen, many different types (modalities) of biometric are available such as face, fingerprints, iris or others. Each has different characteristics and requirements. Determining which modality – or modalities – are required for a new system may be a complex decision. Will requirements change, for example, adding a further modality during the life of the system? Is the simultaneous processing of multi-modalities (multi-modal biometrics) required? Similarly, it is important to judge the proportionality of using multi-modal biometrics against the use case and benefits of adding additional system complexity.

Standards

There are many complex standards relating to biometrics and the relevant ones need to be understood. Compliance with relevant standards delivers important advantages – the interoperability of data and systems; the faster and cheaper development of solutions; lower lifetime cost (initially and when upgrading the solution); interchangeability of components; easier and better testing. In a broader context a 'standards'-based approach also includes professional learning and norms, and consistency in the uses of technical vocabulary to improve communication. Your industry partners will be able to guide you through the complexities.

Accuracy and quality

Achieving high accuracy and high quality biometric samples recorded on a system is critical to obtaining reliable results when using the system. The enrolment of each record is a vital step – if the quality of samples captured and stored is poor, results will be compromised while that system and data remain in use. Accuracy, including measuring False Accept Rate (FAR) and False Reject Rate (FRR), is key and should a result prove inaccurate, it is possible to cascade down from a facial biometric to fingerprints etc. As this paper has noted, additional modalities alone do not guarantee a greater degree of accuracy. Many other considerations also affect the outcomes.

Algorithms

The algorithms used to capture, encode and compare biometrics have an important bearing on how well and how efficiently the system will perform, how flexible the system will be (for example in handling biometric samples or images that are significantly degraded), and in being able to detect attempts to deceive (or 'spoof') the system by presenting a false biometric sample or image (Presentation Attack Detection (PAD)).

Testing

Testing a biometric system is critical. For larger systems it can be a major undertaking. Testing is not just something undertaken as a final stage but begins with a sound strategy related to the circumstances of the system being created, how to prove that it works as intended and delivers acceptable accuracy for all its use cases. Significant quantities of test data may be needed and must be created or built. How will the quality of the system continue to be proved during its lifetime?

Performance

How will the size of the system grow over time? Searching and processing biometric data can be computationally intensive: setting up a large biometric database that will be used by many users demanding fast response times, all of which will expand year by year, requires major and efficient processing power. That too needs to be tested and monitored. Cloud services may help in dealing with requirements for flexibility and growth, but there is no 'silver bullet' or easy answer. Again, this comes back to proportionality and the right solution to fit the use case. If vast, highly performant, multi-modal systems are not required to achieve the outcome, then it makes commercial and operational sense to avoid such over-investments.

Change and growth

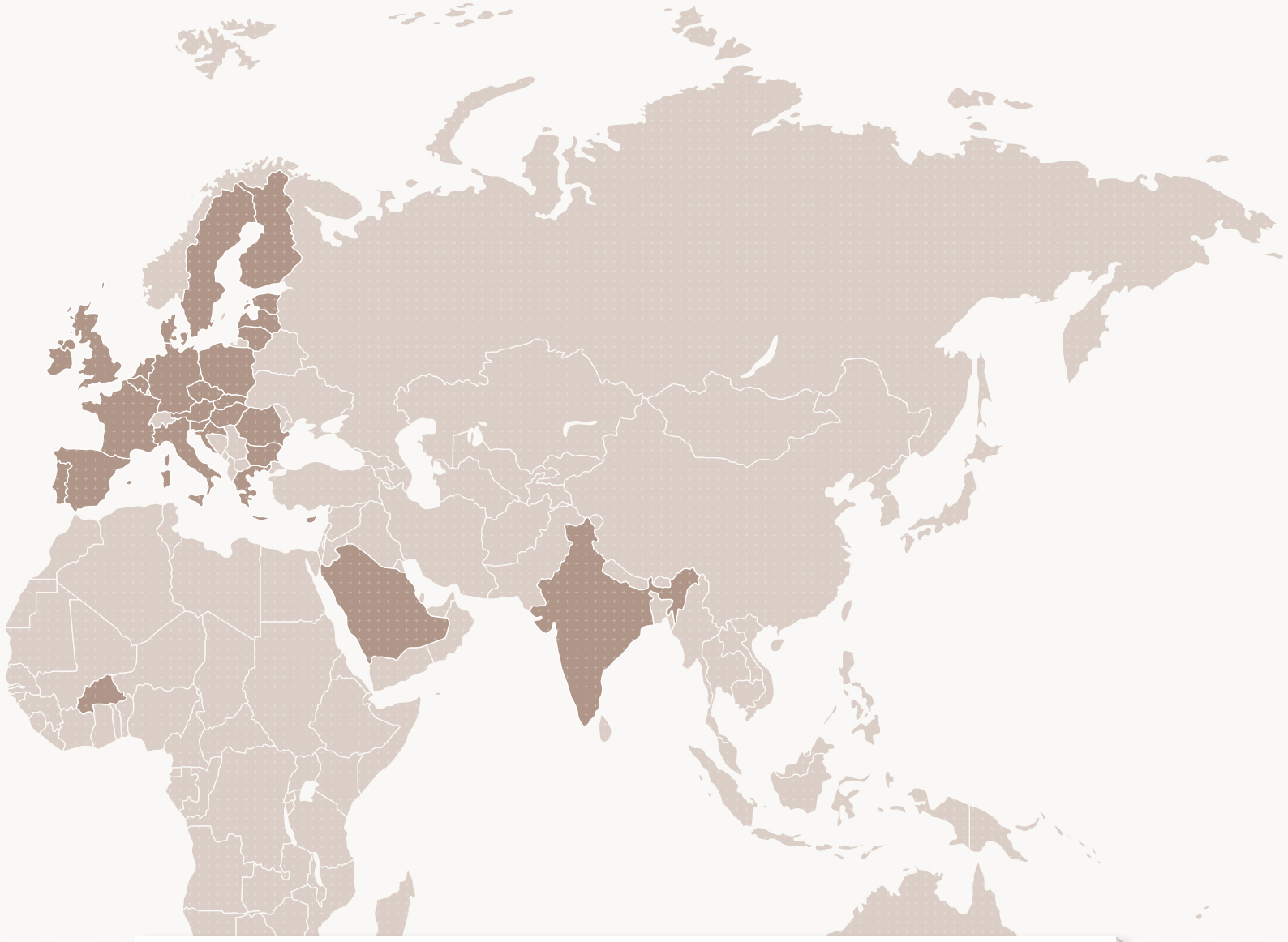
A system is unlikely to remain the same throughout its life. As a minimum there are likely to be new software releases which will need to be adopted; there will probably be growth in the number of records and users to be accommodated which may require by design a comprehensive scalability strategy to grow as it progresses, while there may also be extra requirements that are added after the system has come into use. It is helpful to consider these factors in advance, and to think about how these could be accommodated if and when they are needed.

6. Biometrics Case Studies

6.1 Central national biometric systems

Large-scale national biometric systems that may provide a platform used by other systems

- **Europe:**
  Identity management and shared biometric management system for justice and home affairs across the European Union; UK Home Office biometric programme
- **UK:**
  Home Office biometric programme
- **United States:**
  S-VISIT, IDENT and HART
- **India:**
  Aadhaar national identity system
- **Africa:**
  Burkina Faso voter registration



6.2
More specific biometric systems

Including systems that connect to central national systems for specific purposes

- **UK / France:**
  Seamless rail travel for Eurostar
- **UK:**
  Identity verification for the EU settlement scheme
- **Iceland:**
  EU Entry Exit System
- **EU:**
  Supporting asylum seekers with EURODAC
- **Spain:**
  Streamlined border control
- **France:**
  Entry Exit System
- **Germany:**
  Seamless access control for the Munich Security Conference
- **UAE:**
  eBorders multi-biometric entry/exit
- **USA:**
  Los Angeles secure, seamless biometric boarding
- **Columbia:**
  Immigration gates with iris

6.1
Central national biometric systems - Case Studies

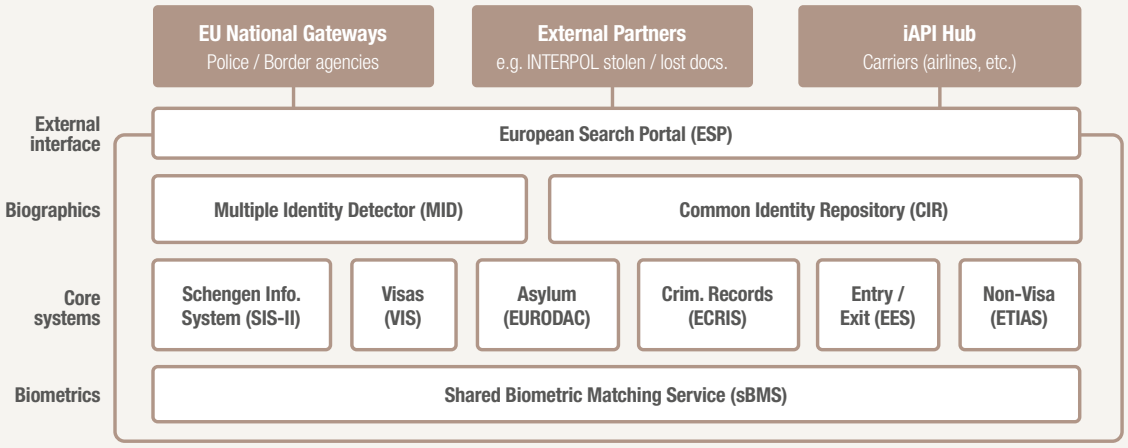
Europe:

EU Identity Management

for Home Affairs and Justice (JHA)

Managed across the EU by the eu-LISA agency, this highly interoperable system in for the Justice and Home Affairs agencies' network is certainly the largest and most complex of its kind in Europe. The diagram shows five core business systems including biometric functionalities already in existence or in development: the Schengen Information System (SIS-II), the Visa Information System (VIS), The European Dactyloscopy System (EURODAC), the European Criminal Records Information System for third country nationals (ECRIS-TCN) and Entry Exit System (EES). The 6th system, European Travel Information and Authorisation System (ETIAS) will enable non-biometric clearance for those Third Country Nationals (TCNs) who do not need a visa to enter Schengen.

The interoperability package reflected on the diagram below is planned to be available by end-2023.



SIS-II
Schengen Information System

VIS
Visa Information System

EURODAC
European Dactyloscopy (fingerprints relating to asylum)

ECRIS
European Criminal Records Information System for 3rd country nationals

EES
Entry Exit System

ETIAS
European Travel Information and Authorisation System

eu-LISA

Europe:

eu-LISA

Shared Biometric Matching System

Managed across the EU by the eu-LISA agency, this highly interoperable system in for the Justice and Home Affairs agencies' network is certainly the largest and most complex of its kind in Europe. The diagram shows five core business systems including biometric functionalities already in existence or in development: the Schengen Information System (SIS-II), the Visa Information System (VIS), The European Dactyloscopy System (EURODAC), the European Criminal Records Information System for third country nationals (ECRIS-TCN) and Entry Exit System (EES). The 6th system, European Travel Information and Authorisation System (ETIAS) will enable non-biometric clearance for those Third Country Nationals (TCNs) who do not need a visa to enter Schengen.

In order to cope with the challenge of implementing interoperability across the different business systems and domains, it was decided to build horizontal identity management services through the implementation of three new applications and their associated databases: the Shared Biometric Matching Service (sBMS), the Multiple Identity Detector (MID) and the Common Identity Repository (CIR). Developed by IDEMIA, the sBMS will contain biometric data templates from all business domains in one central platform with logically separated galleries, exposing biometric search and verification services to the core business systems. CIR will become the central repository for biographic identity data from the different business domains. MID will provide linking services against the CIR and sBMS identity galleries, resolving duplicate and fraudulent identities. Access by EU Member States will be managed via national gateways and the European Search Portal (ESP) to limit access to what is authorised.

How it works

- Ability to ensure the protection of the external borders in the long-term
- Use of the best-in-class European biometric technology
- An accurate, resilient and performant system for all Member States
- Draws on the expertise gained through large-scale solutions that support the European Union, including VIS and Eurodac
- Increased security
- Smoother border clearance process

UK:

Home Office Biometric Programme

The Home Office Biometrics Programme (HOB) develops and delivers capabilities to establish identity using fingerprint, DNA and facial image data, for use by law enforcement and Home Office operations. This includes the provision of a flexible and comprehensive biometric service that will support different user groups, data sets, biometric modalities and stakeholder requirements. HOB is delivering a flexible architecture that provides a common front door, through the Biometric Services Gateway, to the biometric collections they manage, which enables the cross checking of biometrics between the immigration collections and the policing collections for a wide range of operational purposes – including visa applications, criminal arrests and mobile searches by the police and Immigration Enforcement.

The mobile capability, for example, gives a police officer the ability to confirm the identity of an individual through a check of their fingerprints against biometric databases through an app on their police issued smart phone; a mobile peripheral plugged into the smart phone captures the fingerprints (index fingers only) and checks against the biometric databases, police fingerprint collection and immigration fingerprint and face collections, to confirm whether there is a match.

An important element of the HOB Programme is the support it gives to the UK commitment to enhance international data sharing. The Prüm Fingerprint Project is a collaboration between HOB, Home Office Policy, UK policing and the German Bundeskriminalamt (BKA) provides direct access through the HOB Biometric Services Gateway for UK police forces to search against the BKA fingerprint collection and reciprocal searches to be made by the BKA.

The Prüm Fingerprint capability enables the identification of persons of interest in the UK's most serious unsolved crimes, supporting UK Law Enforcement in detecting subjects who have committed offences in the UK or EU, and subsequently enabling investigations and providing valuable intelligence.

Prüm Fingerprint searching went live with Germany in October 2020 and work is ongoing to connect to other EU Member States during 2022. HOB is also working with the Secure Real Time Platform Project (SRTP), to deliver a system that will allow the Migration 5 partner countries comprising UK, USA, Canada, Australia and New Zealand to share immigration biometrics with each other. The SRTP has been developed as the communication component of the Automated Data Sharing solution that will be used to check immigration fingerprints in near-real-time to improve the integrity and security of the border and immigration systems.

Home Office

USA:

US-VISIT, IDENT

and DHS HART

US-VISIT
Keeping America's Doors Open and Our Nation Secure

The United States Real Time Biometric Identification Services **(IDENT)** is the largest biometric border management system in the world, sitting at the heart of the central Department of Homeland Security **(DHS)** system for storage, matching and processing of biometric and associated biographic information. This Automated Biometric Identification System handles digital facial images and 10 fingerprints – taken at ports of entry and consular offices abroad of foreign nationals seeking admission into the United States.

Established in the 1990s, this is a continually growing database that holds over 250 million identities. It is a cross-department approach and combines Immigration and Customs Enforcement (ICE), Customs Border Patrol (CBP), Citizenship and Immigration Services (CIS), and the Department of State. The border system making use of IDENT is **US-VISIT.**

IDENT is currently being upgraded with Homeland Advanced Recognition Technology **(HART)** features to add multimodal biometrics functionality. The upgrade includes a move to a cloud-based solution with large-scale lights-out matching, very fast response time, increased capacity both in terms of total number of records and in number of daily transactions. The new system will include finger, face and iris deployment IDENT is built around an Automated Fingerprint Identification System **(AFIS)** supplied by Thales Cogent Systems.

Key figures

- The largest AFIS in world
- ID checks at 115 airports, 14 sea ports
- Over 250 million unique IDs
- Over 300,000 biometric transactions per day

Benefits

- Helps authorities strengthen homeland protection
- Check the fingerprints of an individual seeking to enter the country against watch lists of known or suspected terrorists, criminals, immigration violators
- Upgrades the largest AFIS in world, to provide multiple biometric support and cloud
- Fast immigration processing at borders
- Security measure to better welcome into the country

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system

India:

Aadhaar

Aadhaar is India's national identity system, the largest such system in the world. Aadhaar means 'foundation', or 'base' and is synonymous with the unique identity number assigned by the system. Aadhaar is intended to provide a universal proof of identity, allowing residents to prove their identity anywhere in the country. Social and financial inclusion is part of the programme aims, enabling access to subsidies, benefits and services, especially for disadvantaged groups.

Since enrolment began in 2010 over 1.27 billion identities have been created, over 93% of the total projected population of 1.36 Bn. Biometrics enrolled on the system comprise facial image, 2 iris scans and 10 fingerprints. An Aadhaar card is available to citizens enrolled on the system, as is a mobile app (eAadhaar). Multiple services have been built on the Aadhaar platform: 256 million Aadhaar identities have been linked to bank accounts, including 20 million through a rapid, paperless facility to open a bank account (e-KYC).

Aadhaar comes under the responsibility of the **Unique Identity Authority of India (UIDAI).** UIADI has created three main 'ecosystems':

- Enrolment and update ecosystem – IDEMIA is organising and delivering enrolments and updates to the system, through registrars, enrolment agencies and operators. Building the database has been a massive task with an average of one-third of a million new identities enrolled per day for more than 10 years
- Authentication ecosystem – a corresponding organisation can authenticate tens of millions identities each day, online and in real time, through service and user agencies, with appropriate technical standards for secure biometric devices. 100,000 or more certified portable biometric devices have been deployed. Banks and payment operators have embedded Aadhaar authentication in micro-ATMs to support banking services across India
- Training, testing and certification ecosystem – this is necessary to support the enrolment and update, and authentication ecosystems

Privacy is a key issue. Despite clear benefits, and important security features, concerns led to a consideration by India's Supreme Court which directed the Indian government to improve safeguards in the Aadhaar legislation.

For more information on UIDAI and Aadhaar see:

Home - Unique Identification Authority of India | Government of India (uidai.gov.in)

Burkina Faso:

Voter Registration

Commission Electorale Nationale Indépendante (CENI) in Burkina Faso requested an upgrade of its voter register, ahead of the presidential elections of October 2020 and legislative elections in March 2021.

The aim of the CENI is to maximise the lifecycle of existing equipment, provided by Thales in 2016 for the voter registry creation, to use it as long as possible. The project successfully achieved two key combined objectives: the re-use and upgrade of existing systems as well as the procurement and integration of brand new equipment to manage a robust voter registration campaign.

Key components

- Refurbishment of 1850 existing kits to start the enrolment early January 2020, with a complete SW upgrade to support new 442 biometric registration process design
- Supply 2850 new enrolment kits to close the enrolment campaign by end March 2020
- Migrate the existing AFIS to Thales AFIS system with an extension from 10 million to 20 million records
- Renew the central IT plus the delivery of training and support for local operations

https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/press_release/thales-helps-electoral-commissions-ensure

UK / France:

Eurostar:

Seamless Travel Trial at London St Pancras International

World-first for rail industry enables travellers to complete ticket and passport checks securely at home

The Eurostar SmartCheck contactless fast-track service enables passengers to enrol remotely and complete secure ticket verification on their mobile devices prior to travel from London St Pancras to destinations in France or elsewhere in the EU. Selected ticket holders can scan their identity documentation using their smartphones, complete a brief biometric face scan to verify that they are the genuine holder of the identity document. The document is authenticated, and the traveller's Digital Travel Credential (DTC) is stored securely on their device within a matter of minutes. Once enrolled, their Eurostar train ticket can be linked, and they are ready to travel.

On arrival at St Pancras International station, passengers proceed through a dedicated SmartCheck biometric lane. A face scan at the ticket gate verifies that the customer has completed the ticket check, with no presentation of paper or electronic tickets needed. A second face scan allows the system to verify that the passenger has submitted correct passport information, which Eurostar then shares with UK Border Force to create a record of exit from the UK.

Solution overview

- More than 50% of the trial participant goal have already travelled through SmartCheck, even with Covid restrictions affecting travel
- Optical character recognition (OCR) of the MRZ in a passport.
- Near field communication (NFC) to access and verify chip data and validate the document
- A liveness test to ensure that a real, live person is genuinely present
- Facial matching to compare a selfie with the chip image and a still from the liveness to assess the alignment of the identity and the person
- Eligible passengers associate their digital identity with their ticket
- An ICAO-compliant DTC is derived and securely stored on their smartphone
- A dedicated biometric lane uses facial verification to check in the passenger with Eurostar. Eurostar then sends the passport data to UK Border Force for an exit check
- Solution provided to Eurostar with the support of Innovate UK
- Delivery by iProov in cooperation with WorldReach Software, an Entrust Company, and Face4 Systems

UK:

UK Home Office EU Settlement Scheme:

Identity Verification Service

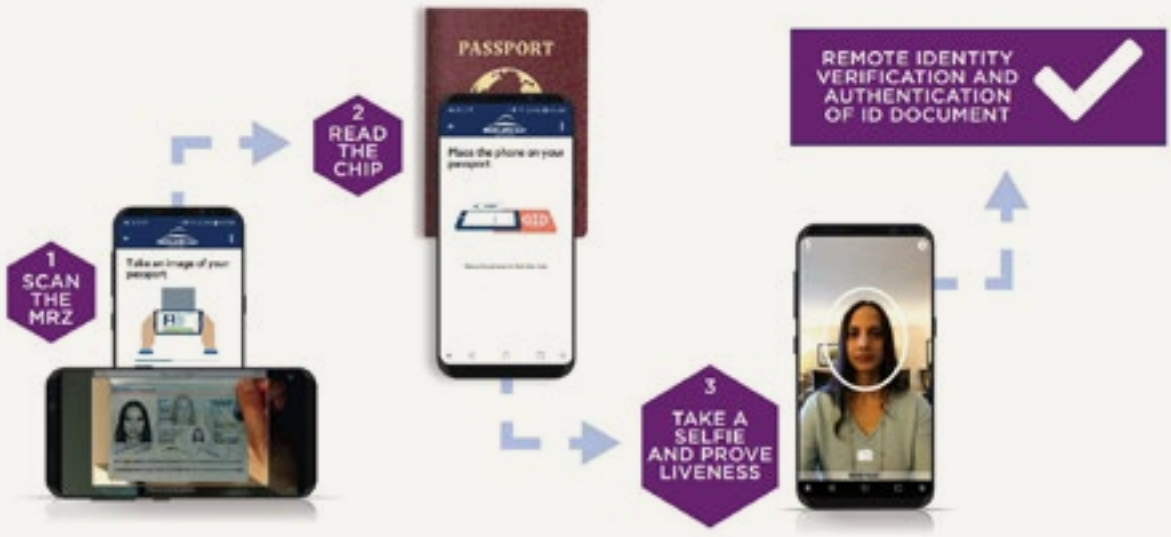
To support the United Kingdom's exit from the European Union, the EU Settlement Scheme (EUSS) was established by the Home Office to allow EEA nationals living in the UK to apply for a UK immigration status. The Home Office sought out new capabilities to include an optional end-to-end digital application channel for applicants.

Entrust (formerly WorldReach Software) was selected to support the identity and document verification (IDV) components of the EUSS through the development, integration, and testing phases. The "EU Exit: ID Document Check" app assists applicants in remotely and securely confirming their identity without the need to submit documents to the Home Office by mail or in person. The service supports multiple eIDs, including ePassports, UK biometric residence permits, and EU citizen eID cards, all using ICAO standards.

"The scheme is the biggest of its kind in British history."
Kevin Foster, Minister for Future Borders and Immigration, UK Home Office.

Solution overview

- Optical character recognition (OCR) of the MRZ in a passport
- Near field communication (NFC) to access and verify chip data and validate the document
- A liveness test to ensure that a real, live person is genuinely present
- Facial matching to compare a selfie with the chip image and a still from the liveness to assess the alignment of the identity and the person
- More than 85 percent of applicants chose the digital route to prove their identity
- More than 6 million applications were concluded by the end of 2021
- A high percentage of applicants completed their application with a high level of identity assurance in under 10 minutes
- During the busiest periods, the service has processed up to 40,000 transactions per day
- Used on over 3,200 make and model combinations of smartphones
- Uptime of this mission-critical service exceeds the SLA
- More use cases added since 2020 include selected student and work visa applications



Iceland:

European Entry/Exit System

IDEMIA has been selected by the National Commissioner of the Icelandic Police and Isavia, operator of Keflavik, Iceland's main airport and other airports to provide a comprehensive border management system for all air and sea border crossing points, including new equipment.

Backed by this new system, Schengen Member State Iceland will comply with EU Entry/Exit System (EU-EES) regulations. The system will manage an average of 10 million travellers per year with manned and automated controls underpinned by biometric technology.

Security and convenience at the heart of the Icelandic project

During 2022, new EU-EES regulations will require that biometric data, including face and fingerprints, of Third Country Nationals (TCNs) be captured and identified at the Schengen Area's external borders. This will affect border check processes for all Schengen Member States.

With 20%-a-year air traffic growth (prior to Covid-19), Iceland planned to implement a programme to manage increased passenger flows primarily in Iceland's main international airport Keflavik, where 95% of the country's largely non-EU arriving and exiting passengers pass, and also in the country's 30 seaports which are defined as external sea border crossing points. The new border management systems and equipment will also contribute to inland control within the Schengen Area.

Iceland, innovation partner in border management

The solution will use advanced technology to upgrade Iceland's border security, contributing to more secure external borders and optimising the passenger flow by complying with EU-EES regulations. Icelandic border crossing points will be equipped with its TravelKiosk™ EU-EES, and automated TraveLane™ eGates, boosting the throughput and convenience of passengers. The end-to-end solution will also include operator-manned counters, mobile solutions and tracking systems to meet the requirements of the Icelandic Police, shortening response times and improving coordination.

Benefits

- Custom-made, future-proof solution presented in an attractive design
- Higher passenger throughput of arrivals and departures
- Increased security, with state-of-the-art anti-spoofing and best-in-class capture and matching
- Effective use of resources
- Faster border clearance process at airports and seaports
- Intuitive, effortless biometric capture
- Increased convenience and satisfaction
- Respect of privacy - GDPR compliant

EU:

Supporting Asylum Seekers with Eurodac

The European Dactyloscopy System (Eurodac) is the EU's asylum fingerprint database. It contains the fingerprints of all asylum applicants from each Member State, as well as fingerprints from those apprehended in an irregular border crossing. Its primary role is to assist in determining the Member State responsible for examining an asylum application made in the EU and to implement the "Dublin Regulation".

Eurodac was the first biometrically enabled system commissioned by the European Union, and the first multinational biometric system in the world. The system captures and enrols all ten fingerprints, the state sending the data, the place and date of the international protection application, together with the individual's gender and a reference number.

In response to the EU migrant challenge, proposals are now being considered by the European Parliament to increase the information stored in Eurodac about individuals, for example in order to assist in reuniting family members.

Where Eurodac differs most from many other AFIS systems is in its unique workflow requirements which are designed to ensure that only Member States can change or read their own records, while ensuring that individual freedoms and rights are protected in the event of an individual being granted asylum or citizenship of a Member State.

Eurodac in figures in 2020

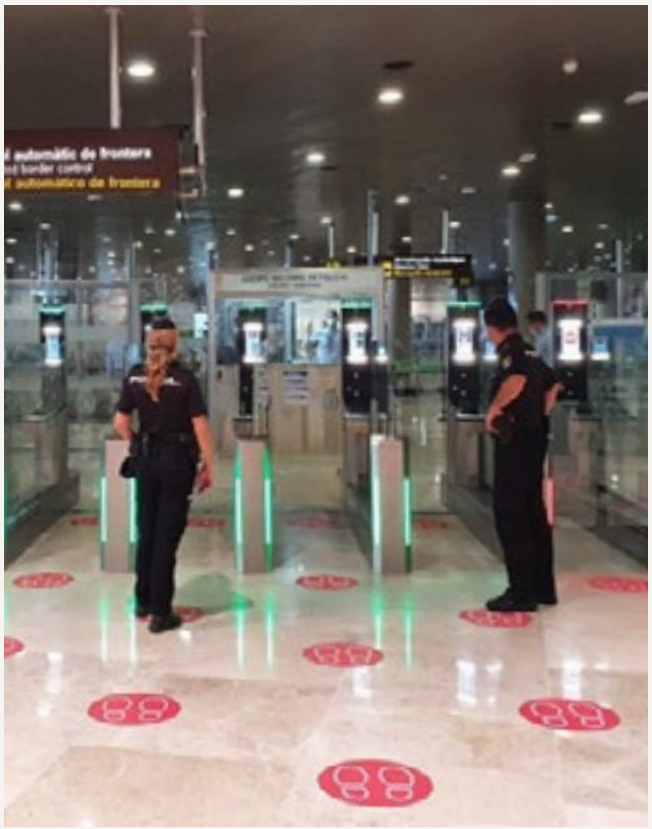
Eurodac usage overall decreased by 30% compared to 2019, mostly due to the reduction in border checks and travel restrictions imposed in 2020:

- At the end of 2020, Eurodac stored more than 5,8 Million fingerprints data sets
- In 2020, 644,926 sets of fingerprints were transmitted to the Eurodac Central System
- Asylum seekers: 401,590 category 1 data sets were transmitted to Eurodac, representing 62% of the total data
- Searches for illegal stays 1: 60,843 category 3 data sets transmitted, representing 25% of the traffic
- Irregular crossings 82,285 category 2 data were transmitted, accounting for 13% of the total transactions

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/eurodac

Spain:

Streamlined Border Control



AENA, the Spanish operator, has entrusted Thales for the supply and deployment of ABC gates latest-generation at six international airports (Valencia, Fuerteventura and Bilbao, Reus, Girona and Tenerife).

This large-scale project represents more than 120 ABC Gates, integrating the latest Thales technologies, including the Thales Cogent FRP biometric facial recognition "matcher" SDK.

These new smart accesses have already been in operation since July 2019 at the Valencia and Bilbao Airports, optimising access time for passengers. The system is key for National Police officers since it facilitates the operation and control of up to 12 passengers simultaneously.

These improvements have been achieved without lowering security as the smart access is provided with facial recognition software that verifies the passenger's identity. Moreover, the units are designed in such a way that the passengers intuitively look at the camera during the process, enabling instant capture of their face.

Automated controls provide speed, improving performance and increasing border security by performing biometric identity verifications against police and international databases such as Interpol.

Key components

- 121 Gates across 6 international airports
- Biometric controls for entry & exit using Biometric Passport or the Spanish biometric Identity card
- Face and fingerprint biometric modalities
- EES compliant ABC gates

https://www.thalesgroup.com/en/group/journalist/press-release/thales-and-inetum-deliver-smarter-border-management-spanish-valencia

France:

Ready for the New Schengen Area Entry/ Exit System (EES)

In March 2021 the French Ministry of Interior selected Thales to prepare France for the New Schengen Area Entry/Exit System (EES). In 2022 Member States of the Schengen Area will be required to have a biometric entry and exit system to register non-European citizens crossing an EU external border. The French Ministry of the Interior will deploy 250 pre-registration border kiosks at various border crossing points. Therefore, France will be equipped with a state-of-the-art biometric solution to streamline and secure its air, land and sea border crossings.

Providing a self-service, intuitive and interactive terminal to guide travelers through every stage of identity registration and verification, the border kiosks will incorporate various document verification and biometric face and fingerprint technologies with face and utilise software optimised for ultra-rapid checks of a document's authenticity and intelligent detection of any attempted identity fraud. They will offer rapid registration for travellers, highly accurate identity verification, data management protection and advanced operational fluidity at border crossings

Key components

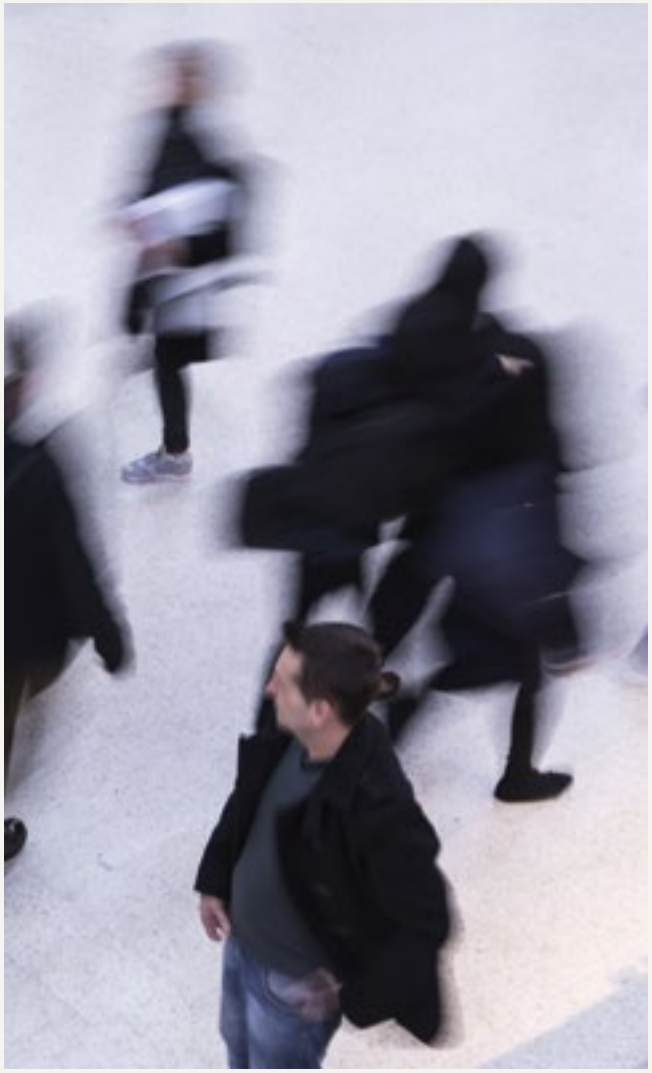
- 250 Border Kiosk in Phase 1
- Document Authentication
- Face and fingerprint biometric capture
- EES compliant
- Connection with checklists and EU ESS database

https://www.thalesgroup.com/en/group/journalist/press-release/thales-selected-prepare-france-new-schengen-area-entryexit-system

Germany:

Reliable and Seamless Access Control

Verifying Visitors' Identity at the Munich Security Conference



The Munich Security Conference (MSC) is a high-level annual conference that brings together key decision-makers from the international security community. Since 2019, the walk-through portals allow for seamless entrance and visitors' identity verification software that reads badges on-the-move. The technology improves verification, speed, and convenience: badge holders only need to step through a portal and their information is immediately verified through an advanced biometric face recognition technology.

Verification of the badges can also be carried out by specialised handheld RFID readers and smartphones, which then show the security personnel the previously provided picture of the participant for manual verification. Using this technology, verification times were significantly reduced and the traffic flow improved without any bottlenecks.

The solution is based on secure ultra-high frequency RFID. It allows only authorised devices to read the high-security contactless chips at a short distance. The result is a state-of-the-art authentication technology that has been successfully introduced at the MSC and that can be implemented in various situations that require reliable and yet seamless access control.

More information at

https://veridos.co/eAccessMSC

UAE:

eBorders (Multi-Biometric Entry/Exit Programme)

UAE engaged IDEMIA to launch an advanced, multi-modal eBorders management programme. With the government targeting economic diversification and promoting the UAE as a centre for global trade and tourism, effective and efficient border management is becoming increasingly vital.

In 2011 the UAE Ministry of Interior (MOI) and IDEMIA, through the joint venture EIMASS, launched the multi-biometric eBorders project at Abu Dhabi Airport to increase border security while improving the passenger experience and throughput. Success led to its extension to the country's four other international airports in 2014.

The MOI wanted to include face, iris, and fingerprint biometrics in the UAE's eBorders project to ensure maximum security at the border while offering a seamless experience to travellers.

Key components of the UAE solution:

- E-registration stations: located in dedicated offices across the country, these allow multi-biometric capture, identity verification, and background checks for citizens and residents who wish to register to use Automated Border Control (ABC) eGates but have never used the eCounter at the airport
- Automated Border Control (ABC) eGates: allow passengers to walk quickly and effortlessly through border control without the need for human inspection.
- E-Counters: semi-automated border control counters at the airport used to register all passengers and make them eligible to use ABC eGates in the future
- Face, iris and fingerprint biometric modalities
- Back end system: manages the data flow between eCounters and eGates. The back-end system also monitors and administers the entire entry/exit system. With an integrated traveller database, it interfaces with the Ministry of Interior's systems for background checks in national law enforcement databases. The system is replicated locally at each airport to guarantee 99.9% availability at all times

Taking care of global travelers and different cultural norms

The UAE wanted the border crossing experience to reflect the warm welcome and hospitality of the country to its many kinds of visitors. Contactless biometric capture and accessibility features at each step in the process provides a hygienic, touchless solution that complies with many cultural norms while being accessible to children and people with impaired mobility.

USA:

Los Angeles Airport:

Secure, Seamless Biometric Boarding

IDEMIA is facilitating a facial recognition system to help US Customs and Border Protection (CBP) increase air passengers' security and border control at Los Angeles International Airport (LAX), one of the busiest airports in the world. The technology has been deployed in LAX's new West Gates at Tom Bradley International Terminal and is a one-stop safety solution for passengers, airlines, and airports alike.

The deployment is part of a contract awarded by Los Angeles World Airports (LAWA) to EASIER, a specialist in e-gate technology. In alignment with protection measures defined by the US Congress, passengers will now get to experience a faster, more accurate, and touchless boarding experience.

In May 2021, LAX deployed 76 self-service biometric e-gates featuring Idemia MFACE technology. These gates allow passengers to board a flight and clear CBP emigration checks via facial recognition. The solution integrates facial image capture with the US Department of Homeland Security's Traveller Verification Services (TVS) in support of international departing flights.

Project scope

- Biometric boarding in a single step – no need to present documents for boarding (passport or boarding pass).
- For airlines that cannot process biometric data, the solution processes passengers in a two-step process where MFace validates passenger emigration checks via facial recognition, and the passenger uses a traditional scanner for their boarding pass.

The solution comprises

- eGate: single door, uni-directional
- Interface to TVS facial departure system, as well as Airline Departure Control Systems (DCS)
- MFACE walk-through face-recognition device

Customer benefits

- Faster and simpler processes at boarding
- Meets legal requirements for US exit regulations
- Improves national security
- Effective, automated, modern solution
- Pleasant boarding experience
- Effortless, non-intrusive: walk-through facial capture

Colombia:

Immigration Gates with Iris

In 2018, as part of an initiative to deliver a state-of-the-art immigration experience at Bogata's El Dorado International Airport, Migración Columbia, the migratory control entity of Colombia, piloted an automated, iris-based, traveller verification system. Columbian citizens enroll before they travel, and on return to the country, the iris reader authenticates their identity and allows them through the barrier.

The Colombian Migración expanded the implementation in 2020 with the Biomig Project at El Dorado International Airport where ABC Iris solution processed and authenticated the identity of more than 700,000 Colombian citizens as they entered the country. During phase two of the project, additional BioMig eGate stations were deployed, allowing travellers exiting the country to also have access to speedy, frictionless border crossing services. In addition, BioMig services were extended to foreigners who reside in Colombia.

How it works

- Columbian citizens register to participate in the program before travelling
- Scan iris at one of 30 BIOMIG migratory control stations
- Unique iris scan is registered with Colombia's Border Management System (BMS) in under 1 minute
- Travellers' data is instantly verified, and identity is compared against databases from Interpol, national police records and other government authorities
- On return, travellers enter national ID number on a touchscreen terminal and glance at the iris scanner
- Identity is authenticated via a secure digital process and again compared against multiple databases
- Automatic doors to swing open and travellers are free to enter Columbia

Key components

- 25 gates
- Iris biometry Solution and gate software integration
- Enrolment integrated with Border

Benefits

- Simplify immigration procedures while improving ease, speed and convenience for end users with ABC Iris recognition solution
- Without compromising security, Colombian citizens can now benefit from strong biometric security within a trusted environment
- Passengers enter their flight number and look at the camera and are processed in less than 25 seconds
- Fewer lines, faster re-entry, and increased passenger satisfaction

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/biometrics-colombia

7. Annexes

Glossary

ABC	Automated Border Control (e.g. e-Gates)
ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
AML	Anti-Money Laundering
ATM	Automated Teller Machine (cash dispensers)
Crore	10 million, in the Indian numbering system
DHS	Department of Homeland Security (US)
DTC	Digital Travel Credential (ICAO)
EES	Entry Exit System (EU)
EU	European Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
FAP	Fingerprint Acquisition Profile, representing the capability of optical devices used for fingerprint capture
FAR	False Accept Rate
FP	Fingerprint
FRR	False Reject Rate
FR	Facial Recognition
GDPR	General Data Protection Regulation (EU)
ICAO	International Civil Aviation Organisation
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
KYC	Know Your Customer, or Know Your Citizen
MAD	Morph Attack Detection
ML	Machine Learning
MRZ	Machine Readable Zone (on the biodata page of a passport)
NFC	Near-Field Communication
NFIQ 2	NIST Fingerprint Image Quality – a quality assessment tool
NIR	Near Infrared (light frequency used in iris recognition)
NIST	National Institute of Standards and Technology (US)
PAD	Presentation Attack Detection
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
SSI	Self-Sovereign Identity

References

[REF1] **Core Principles on Identification for Sustainable Development,**
endorsed by 30 organisations, 2021 edition.
www.idprinciples.org

[REF2] **Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration,**
Patrick Grother, Austin Hom, Mei Ngan and Kayee Hanaoka, NIST Interagency / Internal Report (NISTIR) 8381, July 2021.
https://doi.org/10.6028/NIST.IR.8381

[REF3] **Contactless Travel in Post-COVID Times: Enhancing the EU Security Ecosystem,**
Virtual Industry Roundtable, eu-LISA, June 2021.
https://www.eulisa.europa.eu/Publications/Reports/IR_2021-06_Report.pdf#search=Industry%20roundtable

[REF4] **Biometric Payment Cards - The Next Evolution in Secure Contactless Transactions –**
A Smart Payment Association paper, December 2021.
https://smartpaymentassociation.com/index.php/publications-smart-payment-association/position-papers-smart-payment-association/entry/biometric-payment-cards-the-next-evolution-in-secure-contactless-transactions-an

[REF5] **EES Working Group on ICT Solutions for EU External Borders,**
eu-LISA, March 2019.
https://www.eulisa.europa.eu/Publications/Reports/WG%20on%20ICT%20Solutions%20for%20External%20Borders%20-%20Report.pdf

[REF6] **NFIQ 2, NIST Fingerprint Image Quality,**
Elham Tabassi et al, NISTIR 8382, July 2021.
https://doi.org/10.6028/NIST.IR.8382

[REF7] **Artificial Intelligence and Large-Scale IT systems: Opportunities and Challenges.**
Report of Industry Roundtable, eu-LISA.
November 2021.
https://www.eulisa.europa.eu/Publications/Reports/IR_2021-11_Report.pdf#search=Industry%20roundtable%202021

[REF8] **Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, Report,**
Patrick Grother, Mei Ngan and Kayee Hanaoka, NISTIR 8238.
https://doi.org/10.6028/NIST.IR.8238

[REF9] **NIST Face Recognition Vendor Test, Part 3: Demographics Effect**
Patrick Grother, Mei Ngan and Kayee Hanaoka,
NISTIR 8280, December 2019.
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[REF10] **Privacy by Design: the 7 Foundational Principles,**
Ann Cavoukian, Office of the Information and Privacy Commissioner of Ontario, 2009,
revised January 2011.
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[REF11] **Facial Recognition: It's Time for Action,**
Brad Smith, Microsoft, 2018.
https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action

[REF12] **Guidelines on Facial Recognition,**
Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing, Convention 108, Reference T-PD(2020)03rev4,
28 January 2021.
https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

[REF13] **Facial Recognition Technologies: What's at Stake, and Why?**
SIA blog, July 2021.
https://secureidentityalliance.org/ressources/blog/entry/facial-recognition-technologies-what-s-at-stake-and-why-1

[REF14] **EU proposals for legislation on Artificial Intelligence,**
COM/2021/206, April 2021.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[REF15] **Artificial Intelligence Blog, SIA**
Artificial Intelligence (IA) Technologies:
What's at Stake and Why.
https://secureidentityalliance.org/ressources/blog/entry/artificial-intelligence-what-stake-and-why

Other reports by the Secure Identity Alliance:

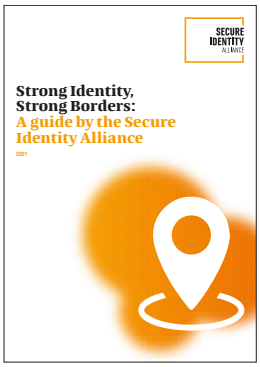
https://secureidentityalliance.org/ressources/publications

Giving Voice to Digital Identities Worldwide

Providing unprecedented 'on the ground' insights and perspectives, the study produced in partnership with onepoint gives a unique voice to stakeholders from 25 innovative sovereign digital ID schemes. Their shared learnings highlight the guiding principles and good practices that are critical for driving usage, adoption, and success – regardless of the digital ID model adopted.

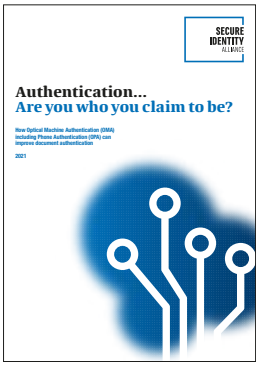
Passport Fraud Trends and Ways to Combat Them

The purpose of this report is to draw a clear link between the problems of document and identity fraud faced by issuing and control authorities, and selected private organizations such as financial services institutions. It also explores some of the technical solutions to those challenges as proposed by the global identity management industry.



Strong Identity, Strong Borders

Looks at the need for border authorities to balance security and protection with efficient and frictionless passenger experiences. In addition to the major drivers shaping the future of the border control space, the report looks at the vital - and complex - role played by identity management, highlighting some of the evolutionary technologies incl. automation, biometrics, mobile, and bringing those solutions to life in the form of case studies from around the world.



Authentication: Are You Who You Claim to Be?

This report from the SIA addresses the challenge of identity authentication. Discussing the inherent difficulty in validating someone's identity, as well as some of the solutions that are currently available, the report also provides detailed use cases and recommendations for anyone who may be looking to improve their understanding of this critical practice.

SECURE IDENTITY ALLIANCE