SECURE IDENTITY ALLIANCE

Strong Identity, Strong Borders:

A guide by the Secure Identity Alliance

2021

Mentions

Secure Identity Alliance (SIA)
www.secureidentityalliance.org

Design
Design Motive Ltd

Photo credits
Shutterstock

Editorial review
Slingshot Communications

Production
This report has been produced by the Border Working Group of the Secure Identity Alliance (SIA).

Members of the SIA Borders Working Group:

Michael Brandeau
Veridos (Chair)

Françoise Bergasse, Roger Edwards
Thales

Emmanuel Wang, Nicolas Phan
IDEMIA

Alejando Pulido
IN Groupe

Christina Schäffler
VERIDOS

Jean-François (Jeff) Lennon
Vision-Box

Andreas Zechmann
OSD

Frank Smith
Advisory Observer to the SIA, Former Deputy Director, UK Home Office (Lead Author)

SECURE IDENTITY ALLIANCE

Contents

The changing face of identity at the border

Effective border control has always relied on strong identity management; as early as 1914 , a photograph of the holder became a mandatory requirement for European passports, with governments across the continent seeking to safeguard their boundaries.

Today, with scientific and technological innovation occurring at breath-taking speed, a wealth of new tools and techniques are helping to fundamentally redefine the nature of identity. Simple photography has been supplemented by new and increasingly incontrovertible ways to prove that a visitor is who they say they are, from biometrics to facial recognition.

Border control is about more than just security, however. While COVID-19 may have disrupted the flow of international travel in the short term, the long-term trend pre-pandemic saw passenger volumes set to double over the next 20 years. Ensuring that genuine travellers enjoy as quick and frictionless a border control experience as possible will be vital to managing the inevitable surge in demand as life gradually returns to normal.

In its role as a not-for-profit global identity and secure digital services advisory body, the Secure Identity Alliance (SIA) is committed to the sharing of best practice in the establishment and evolution of integrated border strategies around the world. As border authorities everywhere strive to balance security with efficiency, this report – published by our dedicated Border Working Group – is representative of that commitment.

Over the coming pages, we explore the key drivers and considerations shaping the border control, as well as successes and lessons from agencies around the world.

1.
Executive summary

Welcome.

This guide provides an introduction to border control for anyone who wants to understand this subject more, but who is not an expert. It is available in French and English, online and in hard copy, from the Secure Identity Alliance (SIA).

Knowing where to start is often a confusing challenge when exploring a new topic. This guide introduces the key concepts that relate to border control and then builds your knowledge and understanding of the key elements that relate to today's modern border control systems.

Border control aims to protect the **security** of the country, using vigilance, skill, information, and technology, to identify people who might not be eligible to enter. However, most travellers are genuine, so border control also aims to **facilitate** their entry, as easily and quickly as possible This both serves the interests of travellers/ passengers and the economic interests of the country.

Section 2 of this guide sets out the context in which border control operates – the main drivers, the role of identity, and examines the COVID-19 global pandemic.

Section 3 describes in more detail a general framework for border control – its aims, how the control operates at the border itself, the broader concept of multi-layer security that starts before the passenger travels, the use of biometrics, privacy, integrating multiple components to deliver modern smart borders, and looks at what is coming further down the line.

Section 4 features case studies – examples of actual border control systems in use around the world in North and South America; Europe; Africa; Asia and the Far East.

Section 5 contains reference material on relevant organisations, and a glossary of terms used in this guide.

We hope you find the guide helpful.

Secure Identity Alliance

2. The Context for Border Security

2.1
Drivers

Border security is an essential task that involves many significant challenges. There are several complex drivers, including:

- **Security** – national borders play a crucial role in protecting a country's security, in detecting and preventing the entry of travellers who may want to do the country harm. This could include crime, terrorism, and people trafficking, as well as individual travellers who may be seeking to work or claim financial support to which they are not entitled. A variety of approaches may be attempted to gain entry to a country, and border authorities need to be alert and able to detect such attempts. The responsibility for border security goes wider than staff engaged at ports of entry and will include agencies that co-ordinate national and international efforts against serious and organised crime, such as INTERPOL. New threats may also emerge.
- **Facilitation** – at the same time, a good border function also needs to be focused on allowing genuine passengers/travellers who do meet the rules to enter the country as quickly and easily as possible, avoiding inconvenience, delay and congestion in the limited space that may be available at an airport. And yes, pursuing security **and** facilitation may conflict – either of these aims may work against the other. Welcome to the complex world of border control.
- **Changes in passenger volumes** – over several years, air travel **had** been steadily increasing, with implications for airlines, airports, border control authorities and others. Around 2016 there was general acceptance of projections by the International Air Travel Association (IATA) and the Airports Council International (ACI) that passenger volumes would continue to increase steadily as a **long-term trend** and would double in the next 20 years. However, this steady state of growth was severely disrupted in 2020 by the global COVID-19 pandemic (see Section 2.3). Significant **short-term** flows can also arise as a result of political instability, armed conflict, economic factors, flood, famine – and perhaps in the future, may arise as a result of global warming. This is a problem not only for border control, but for nation states generally.
- **Technology transition** – the digital revolution involving the internet, mobile devices, online payments and online access to government and commercial services is still evolving. New technology innovations are being developed to assist border security that build on existing achievements with biometrics - ePassports, eGates, Advance Passenger Information, visa waiver and/or travel authorisation schemes and others. This evolution represents both an opportunity and a challenge; while offering the opportunity for improvement, any change implementation will come with associated risks and the possibility of disruption or failure.
- **Global context** – all of this is taking place in an increasingly interconnected world. As a result, there is a need for international co-ordination, agreements, and standards plus a recognition that inconsistencies between different national approaches, priorities and laws will need to be managed.

2.2
Strong identity – a key part of the picture

Identity is central to border security, as highlighted in the framework contained in Part 3 of this guide. When a passenger arrives at a border, the border officer wants to see evidence of that person's identity (a passport or identity card) and to verify that the person, the travel document, and the identity presented all match. Biometrics can be used to verify identity either by a visual comparison of the passport photo and the person presenting it, or an automated check at an eGate or self-service kiosk. Biometrics are also used to enrol an applicant's fingerprints and facial image for a visa, to check their identity against records already held, and to verify this is still the same person when the traveller presents their visa and passport at the border.

The need for effective use of identity to safeguard border security complements the effective use of identity in recording evidence of a country's citizens through records of birth, marriage, and death; and in scrutinising applications for a passport. Technology plays an important role in enabling and assuring evidence of identity processed in these ways, and increasingly involves the use of technology that is directly accessed by the citizen and even carried with him or her in an eiD card or smartphone.

Having the capability to analyse large volumes of data and link information relating to the same person, supported by biometrics where relevant, to form a holistic person-centric view of an individual, accurately, across multiple sources, in real-time, and supported by proper evidence – is important for delivering effective security and facilitating entry into a country for genuine passengers.

As these systems continue to develop, the processing of increasing amounts of personal information highlights the importance of safeguarding individuals' privacy, in accordance with the law, and ensuring access to benefits due to the citizen by the state – all of which are important aspects of the good use of identity.

The Secure Identity Alliance (SIA) works with governments and agencies across the world to promote the effective use of identity in all contexts.

2.3
COVID-19 global pandemic

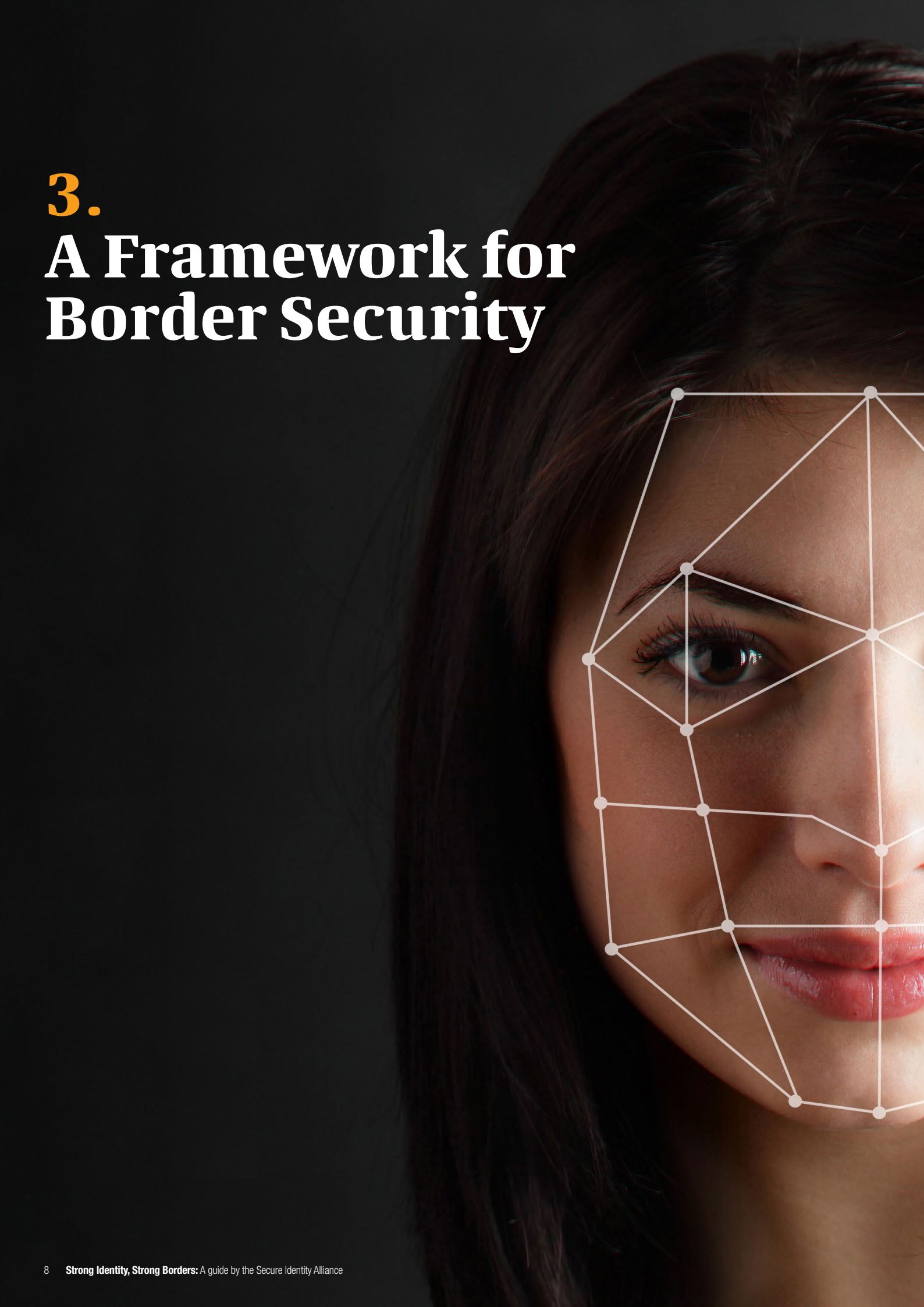
It looks increasingly likely that the credentials required of today's travelers will evolve to include (or be helped by) the secure certification of their health status. At the time of writing (Q1 2021) a wide range of potential systems are under development – although it remains to be seen which standards and solutions gain widespread acceptance in the market.

While the role of these so-called 'health passports' is an important step in re-establishing cross-border travel, there are significant technical, operational and commercial complexities to overcome. In recognition of this, and of the global nature of the challenge, the SIA strongly advocates the need for solution interoperability, the re-use and adoption of existing standards, and close international collaboration and co-creation.

Given how pervasive and fast-spreading COVID-19 is, it is not only vital we move rapidly to address the problem today, but also consider long-term measures to combat new threats as the virus mutates. Similarly, having experienced the shock of COVID-19, it is critical we learn lessons and are able to adapt solutions and approaches to target any future **new pandemics.**

Strong identity leading to strong and efficient borders can play a major role in ensuring that those who enter or exit a country are safe, in terms of security and health, thus supporting the re-launch of the economy and regular trade, following the pandemic. The trusted combination of strong identity, normalised biometrics and accredited health data may become one of the pillars of re-building trust in travel, and indeed foster economic recovery and trade at the borders, through the usage of government issued digital identity wallets.

3.
A Framework for Border Security



3.1
Aims, strategy and implementation

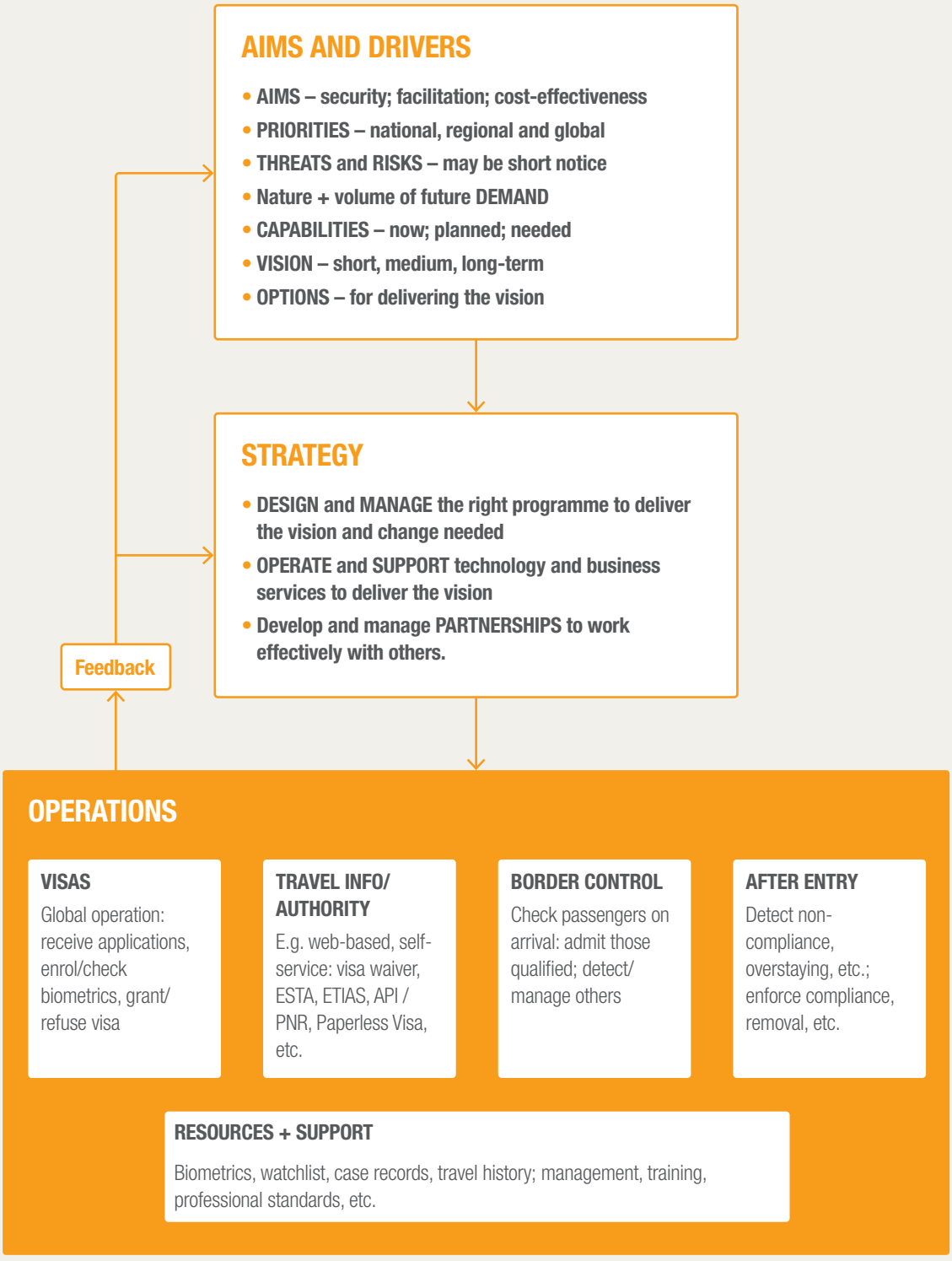
Section 2 of this guide discussed the context of border control, including the key aims of security and facilitation; the effect of the COVID-19 pandemic; and the importance of managing identity in this (new) world.

While there is no single universal solution, as circumstances vary considerably between countries, **Figure 1** sets out a generalised **framework for border control**. This suggests a cascade starting from the **aims and drivers** – the underlying aims and purpose of border control; an overall **strategy** for realising these; and border control **operations** – the 'engine room' comprising systems, processes, people, and data that will deliver the strategy and therefore the aims.

- **Cost effectiveness** – no country has limitless resources with which to create the 'perfect' border control solution and a balance needs to be made between security, facilitation, and the resources the country can allocate. This implies consideration not just of cost alone but also the effectiveness and benefit that will be derived; traditionally this is set out in a business case that makes a reasoned conclusion on what is right to do.
- It is good to consider solutions others have adopted, but it is still important for each country to decide **what is right for their individual case**. The model outlined at Figure 1 below offers an a la carte menu of possibilities, but it is up to each country to decide on the balance of security, facilitation and cost effectiveness that is implemented - and the technologies and business processes adopted to deliver this, preferably delivering value for money.
- Devising the right strategy can be **difficult** and **challenging** when set against the conflicting pressures of financial constraints, legacy IT systems, demands for high quality services, new and unpredictable threats, and political and public scrutiny. This report is a contribution to making sense of this challenge – without suggesting that the answers are easy.
- **Delivery** of the chosen strategy needs to be well-managed. This goes beyond simply making choices about technology and will involve good project delivery and change management; the development of new business processes to make use of new technologies; and the integration of new and old systems and data. **Expertise** from individuals and advisers, along with the exchange of good practice with other border authorities, suppliers, and others, can help to achieve delivery success.
- Border control is never possible in isolation: an effective system will be even more effective when it is delivered in an effective **partnership** with others; for example, airport and other port operators, airlines and other carriers, agencies - including police and customs - countries, and travellers themselves.

Next, we take a more detailed look at the components that go into building the operational capability needed to make the strategy become a reality. This will encompass work at the border, including automation and mobile solutions; multi-layer security; biometrics; change management as well as recurrent training, and a look forward to future approaches and emerging technologies.

Figure 1
Border control: an overview



3.2
At the border

Control at the border – the point where a passenger physically enters the country – is of particular importance. This is where each passenger will show their passport, ID card or other travel document, and the border officer will decide whether to admit the person to the country.

Configuration – the greatest volume of travellers may enter through main air or sea ports or at a main land border, but there are many possible variants including: by foot, by road vehicle, in passenger transport such as coach or train; by tunnel, crossing a water or land border; where passengers enter a common travel area giving open access to more than one country such as the Schengen area in Europe; where by agreement border control is operated at the point of departure rather than arrival (a 'juxtaposed' control); or at very small airfields, harbours or minor land crossings where a full border control may not be practical. Control may also be exercised on a mode of transport, for example, on board a ship, train, or road vehicle.

Critical aspects of control

- The ability to verify a person's identity and eligibility to enter the country requires sufficient **skills** and **training** for front-line officers, together with effective **support systems** and **resources** such as fraud detection, intelligence on matters of current importance, and access to many different systems to check records about a passenger/traveller when more detailed examination needs to be made.
- A critical support system is a **watchlist** for raising alerts about a person or passport (or other travel document) about which there are concerns; for example, because the passport has been reported lost or stolen, or the person is wanted by the police. INTERPOL provides a global Stolen Lost Travel Document (SLTD) database which can be checked in addition to national watchlists, to give extra assurance (see Section 5).
- A passport reader which automatically triggers a watchlist check can also test the cryptographic security features built into the microprocessor chip of the travel document in accordance with the International Civil Aviation Organization's **ICAO 9303** standard (see Section 5) – another important assurance. It is essential to **rigorously** authenticate the chip and the data it contains, using trusted public key encryption certificates from the ICAO's Public Key Directory **(PKD)**.
- To deliver security **and** facilitation efficiently, the border control team needs some capability to vary the scrutiny a passenger is subjected to, taking **risk** into account. Where the officer can quickly decide a passenger is eligible to enter the country, it is important to allow the passenger to enter, and move to the next person; where concerns arise, it is important to be able to take extra time to ask more questions or check conditions.
- A **skilled border officer** can decide how to handle each case, checking multiple issues quickly – is this passport valid or is there evidence of fraud? Does the passport match the person presenting it – using visual inspection and/or automated control, including biometric checks. Does the passenger have evidence to show they can enter the country? Is the passenger credible? Taken overall, does the evidence make a convincing case for this person's entry to the country? Good professional training and support for front-line officers is important.

3.3
Automation

- Automated inspection systems, such as kiosks and eGates, are an established and important component of control at the border. These use automation to check travel documents; use biometrics to verify the document matches the passenger; and check a watchlist and chip security features. An eGate can be used to admit a passenger meeting specified criteria, and kiosks to pre-screen and register passengers before proceeding to a border officer in person.
- eGates are particularly useful where the tests required can be fully automated; for example, where nationality is enough to qualify for entry, or the passenger has pre-enrolled as with a trusted traveller scheme; and where subjective questions do not need to be asked. eGates can also be used for embarkation (out-going) passengers.
- eGates can therefore focus particularly on lower risk, easier to process passengers, allowing skilled border officers to be used on higher risk and more complex cases; used effectively these solutions can deliver cost efficiencies.
- There must however be confidence in the system; for example, that the checks undertaken work well and are robust in defending against imposters using the gates or 'spoofing' the biometric verification (see presentation attack detection in Section 3.6 on biometrics, below). This requires good design and rigorous testing – and some operational supervision.

3.4
Mobile solutions

- Mobile devices such as smartphones, tablets, and body-worn video, are increasingly being deployed for front-line tasks in law enforcement, including policing and borders. These devices can provide real-time access to complex IT systems at the front-line, with facilities developed specially for those undertaking these roles.
- Uses for border control can include:
  - » Real-time identification anywhere of people whose identity is in doubt.
  - » Access to supporting information such as reporting immigration status and travel history may be useful; so too is the ability to conduct more detailed 'secondary' examination going beyond initial border control.
  - » Rapid deployment of border control capability to small remote airstrips or ports - locations not normally fully staffed or resourced.
  - » Dealing with mass (irregular) arrivals of passengers or migrants, or disruption or emergencies such as the closure of a terminal at an airport.

3.5
Multi-layer security – exporting the border

- Control on entry to the country is essential, but security and facilitation can be enhanced by additional layers of testing so that a passenger is already known and can have advance checks made to verify their identity, alert border control further in advance of arrival, or be refused entry before boarding an aircraft to travel to the country. **Multi-layer security** of this form is also known as **'exporting the border'**. Examples of how this can be achieved are given below.
- Basic information about each passenger and their travel document – **Advance Passenger Information (API)**, or the more extensive **Passenger Name Record (PNR)** information from the airline's booking system – may routinely be required of carriers to disclose who will travel to the country on each journey. This can be processed by the destination country to check against watchlist information and intelligence, and risk assess information to produce alerts about passengers who may be of interest. This processing may result in refusal of authority for the passenger to travel to the country.
- **Advance online authorisation before travel** can go further in that additional questions may be asked, and an explicit authority may be required before a passenger may board a flight to the destination country. Examples include the US Electronic System for Travel Authorization (ESTA), the Australia/New Zealand Paperless Visa scheme and the proposed EU Travel Information and Authorisation (ETIAS) systems. These schemes can be described as 'visa waiver' schemes. Authority can be checked on arrival but also by airline staff before a passenger embarks an aircraft.
- **Full visa schemes** typically require a face-to-face interview by a representative of the destination country, such as an embassy or commercial partner. These may well include biometric enrolment - of face and fingerprints for example - which can be checked against police and immigration records back in the home country before a visa is issued. This allows for the most rigorous checks in advance, including 'breeder' documents such as birth and marriage certificates and other supporting documentation, but at a higher cost.
- In use cases where biometrics have been recorded in advance, this record can be used to **verify** the person's identity when they arrive in the country – in other words, 'yes, this is still the same person who applied for the visa'.
- Border security alone is only part of the answer. For a border to be effective, other measures must also be effective. That means there needs to be high standards of design and issuance of passport and other travel documents (in all countries, not only your own); good detection of fraudulent travel documents and effective action to tackle the criminal organisations producing these is also vital; and finally, ensuring that once new technical capabilities are provided, these are put to good use operationally and are properly supported.

3.6
Biometrics

- Biometrics refers to the use of identifiable attributes of a person for identification and authentication. This can include different types (or modes) of biometrics, for example facial image, fingerprints, or iris. **Enrolment** is when someone's biometrics are captured to be stored for future reference; **verification** is when a 1:1 check is made against a known record to confirm someone is who they claim to be; and **identification** consists of a **1:many search** when a collection – potentially very large – is examined to try to find a match against one person (identity). These operations can use a **single** biometric mode, or **multi-mode** biometrics such as fingerprints + face + iris.
- **Multi-mode biometrics** can potentially allow faster and more accurate searching of a large collection; can be more robust in finding a match if some data is incomplete or poor quality; or enable a link to other systems where different biometrics have been stored.
- A substantial body of **good practice** and **technical standards** exist for biometrics. The rigorous **design** and **testing** of biometric systems by experienced **experts** is essential and will be needed throughout the lifecycle of a biometric system, from the outset.
- Traditionally, fingerprinting has been associated with **policing and crime**, resulting in caution and sensitivity by the public in relation to allowing their fingerprints to be recorded. However, the increased use of biometrics as a standard part of the visa process in many countries and for passport issuance in Schengen countries, coupled with the widespread use on smartphones to authorise secure payments, is helping to 're-position' biometrics as a more widely accepted part of **identity assurance** rather than specifically something for criminal investigation (in reality, it has relevance in both).
- The field is still **evolving**. Automatic fingerprint identification systems (AFIS) can search very large fingerprint systems containing 10s or 100s of millions of records in a matter of seconds. Developments are taking place in improving sensor technology and linking biometrics to other records. These developments are important for enabling biometrics to be used in mobile law enforcement solutions and increase the ability to resolve doubts over identity very quickly, in the field. Algorithms have improved, thanks to machine learning. Contactless sensing has increased. Use of biometrics for 'data fusion' with other collections of data can increase the value that can be made of biometric information.
- Application for **border control** can include enrolling a visa applicant and checking with greatly increased certainty whether they have used different identities or have had a criminal conviction or immigration problems in the past against; to verify the same person presents the visa when arriving at the border; to enroll an asylum seeker or someone being deported so that they can be recognised in the future. Biometrics may also support more efficient **airport operation** (see IATA/ACI Smart Security at Section 3.11 of this document).
- Attempts can be made to fool or **'spoof'** biometric technology, for example by presenting forged or false biometric images. Work is therefore being undertaken to make systems resistant against this using 'liveness testing' to check that a biometric image or sample is taken from a real, living person. This topic is known as **Presentation Attack Detection (PAD)**.
- **Legal** aspects must be considered. We have already mentioned the importance of **privacy** in handling personal data – biometric data very much falls into this category.

3.7
The Passenger Journey

Figure 2

3.8
Privacy

Advances in the capability and adoption of technology in the management of borders by official agencies, ports, carriers, and others are increasing the amount of personal information processed. This has real benefits for travellers, who can complete their journeys and enter another country more easily; and for society through increasing the security with which people are admitted to a country. More widely, national identification systems confer important rights and benefits on citizens, supporting inclusion. Nevertheless, citizens have a legitimate interest in what data is held about them, how widely it is shared, whether it is accurate, and how systems are governed – and whether this all keeps up with changes in the technology. Which is why many countries and regions have introduced legislation on privacy. In Europe, data protection frameworks such as the **General Data Protection Regulation (GDPR)** together with recommendations issued by the Council of Europe precisely address the issues of privacy-sensitive technologies in a highly constructive way.

Privacy by Design is a widely recognised framework which can help governments, travel operators and citizens to orchestrate, operate and manage sensitive data under a harmonised and legally sustained basis. It can be used as the basis for certification (gaining confidence by other stakeholders) and has been adopted by IATA's One ID concept.

The seven principles of this framework are:

- Proactive not reactive – preventative not remedial
- Privacy as the default
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifetime protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it open

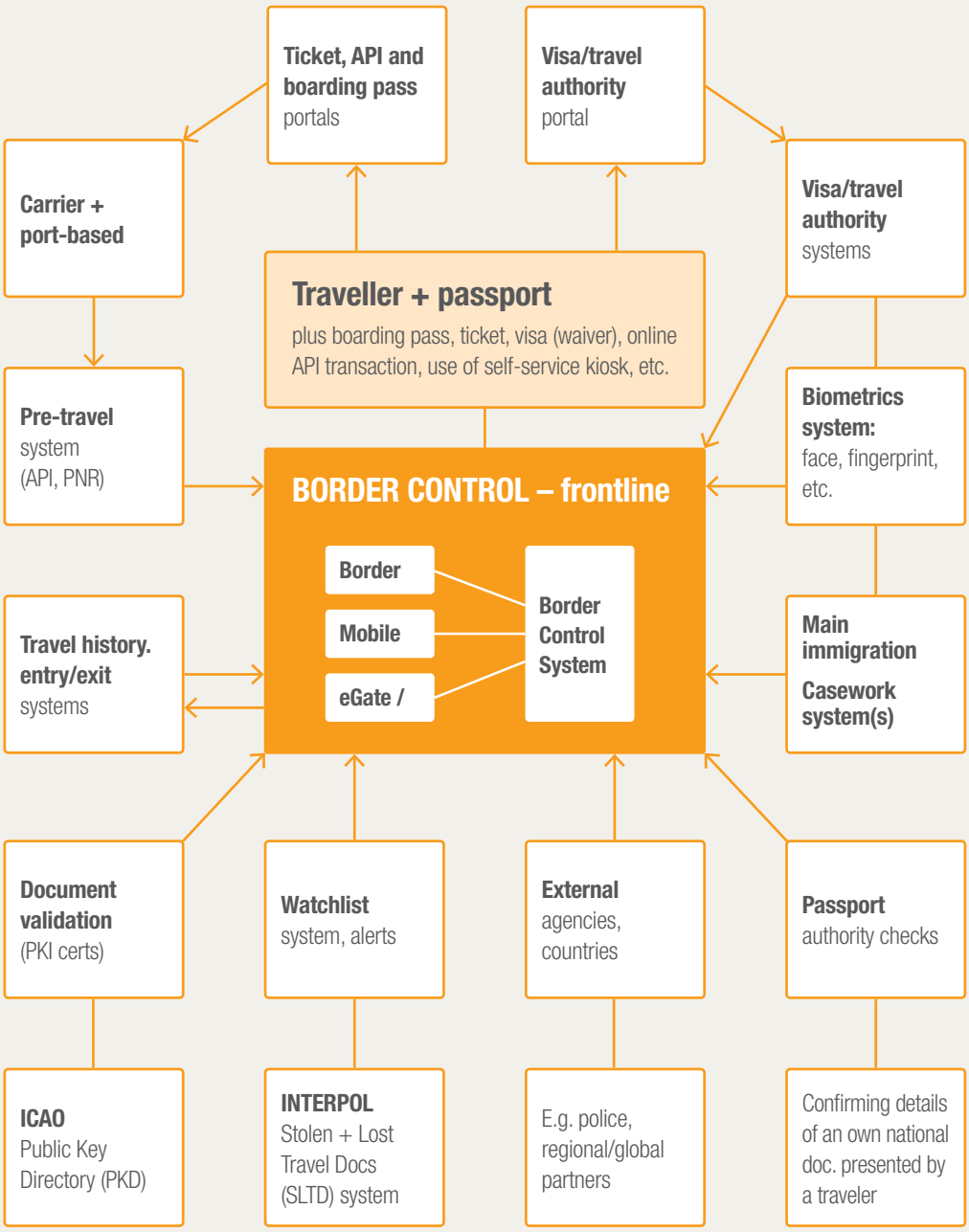
For more details see: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ and https://en.wikipedia.org/wiki/Privacy_by_design

The World Bank Group's Identification for Development programme (ID4D) has published **Principles on Identification for Sustainable Development Towards the Digital Age**, which endorse the need for national identification schemes, and the principles of Privacy by Design. For more information, see: https://secureidentityalliance.org/ressources/blog/entry/10-principles-for-good-id-a-2021-refresh

3.9
High-Level Architecture

Figure 3

This model shows how the elements (people, systems, and data) may connect, focused on the **traveller,** and on **front-line border control**. Systems and interconnections will vary between countries and regions, so this is a **generalised**, indicative diagram: it cannot exactly describe **every** system.



3.10
Smart borders

We have now painted a comprehensive picture of the many elements that may come together to form a complete and effective border system. **Smart borders** is one way of describing such a system where advanced technology components have been used, all of which are well integrated together, to provide a highly effective border system that delivers both security and volume throughput (facilitation).

A good example of the smart borders concept is the modernisation of European Union Schengen border platforms and underlying systems. The core infrastructure and systems are being built for the Schengen Member States of the EU by **eu-LISA**, the European agency responsible for operational management of large-scale IT systems in the arena of Freedom, Security and Justice.

In October 2020, the Executive Director of eu-LISA, Krum Garkov, described the task of bringing this smart borders solution together as an unprecedented challenge. He explained that the EU's transformational approach is to build a unified ecosystem across air, land, and sea, automating routine activities or removing the need for these activities. This will empower human operators, freeing up valuable time to help them focus on important tasks that require specialist training.

The main systems involved are:

- **Schengen Information System (SIS-II)** – which provides real-time alerts on persons of interest to law enforcement, for example at the border.
- **EURODAC** – which records asylum seekers processed in the EU.
- **VIS** – recording visa applications and visas granted or refused in the Schengen free-travel area of the EU.
- **Entry Exit System (EES)** – which will record Third-Country Nationals (TCNs - non-EU nationals) entering and leaving Schengen, ultimately replacing traditional entry and exit stamps in passports with this automated solution. Member States will check TCN travelers into and out of Schengen at fixed and mobile border control points on the Schengen border, using biometric recording and authentication.
- **Electronic Travel Information and Authorisation System (ETIAS)** – recording online authority to enter Schengen given to TCNs who do not require visas.
- **European Criminal Records Information System for TCNs (ECRIS-TCN)**.

Except for ETIAS (an online system for direct access by travellers), the five other systems all depend on a very large and **shared Biometric Management System (sBMS)** which will help to link identities of people on these systems, even though individuals' names and passport numbers may change over time, allowing for identity de-duplication in an interoperable manner.

3.11
Looking forward

There is every reason to expect new challenges to border control will continue to emerge in the future. Fortunately, there are also several new technologies and other solutions being developed to help. Here are some you may expect to see soon.

- The use of **biometrics** and **integration** between passengers, border services and airport operations will increase, as envisaged by the ACI's **Smart Security** and IATA's **One ID** initiatives. According to IATA: "One ID introduces an opportunity for the passenger to further streamline their journey with a document-free process based on identity management and biometric recognition … The objective is to achieve a truly interoperable system coordination between airports, airlines and governments."
- **Mobile solutions** are continuing to be used more widely by the public and by control authorities to deliver ready access to information and services wherever the user needs to be. Rather than at fixed positions. 5G mobile communications will aid this continued development. Identity on a smartphone **(mobile identity)** for international travels, allowing people to assert and validate trusted identity on a mobile device.
- The next generation Logical Data Structure on the **ICAO 9303** secure passport / ID card chip (**LDS-2**) with more memory on the chip holding more data from the issuer and potentially allowing other countries to write data (travel history, electronic passport stamps or visas) securely into the chip.
- ICAO is also developing new forms of trusted identity under the concept of **Digital Travel Credentials (DTC)**. This will comprise a two-part solution of a linked **physical** and a **virtual** component, such as an existing ePassport or mobile phone together with data stored security on the cloud or the device. (See **SIA blog** on this: https://secureidentityalliance.org/ressources/blog/entry/digital-travel-credentials-dtc-the-story-so-far)
- The German Federal IT Security Agency **(BSI)** has recently defined a new Protection Profile (security specification) allowing advanced, secure chips to be certified as being able to hold trusted identity data… such chips could then be included within secure mobile phones. The German government will enable an electronic copy of a citizen's eID card to be copied onto such a phone.
- A smartphone could also hold confirmation of a traveller's **health inspection** (for example, the **CommonPass**, mentioned earlier in Section 2.3 of this guide on COVID-19).
- Biometrics are playing an increasing part in managing identity across multiple, very large databases, so that a holistic, 'person centric' view can be managed of someone's transactions with a border control agency. The EU agency **eu-LISA**, which supports identity systems for law and order across the European Union (EU)'s shared Biometric Management System (sBMS), will link personal records on five major identity systems (see the previous Section 3.10 on Smart Borders). This will support biometric identity checks at the European / Schengen border at fixed and mobile points of entry and exit.
- As the range of information sources and analysis that can be performed at the border increases, so too does the need for the **smart, automated integration** of data with advanced data analytics (big data analysis). Artificial intelligence and machine learning will also boost the development of these solutions.

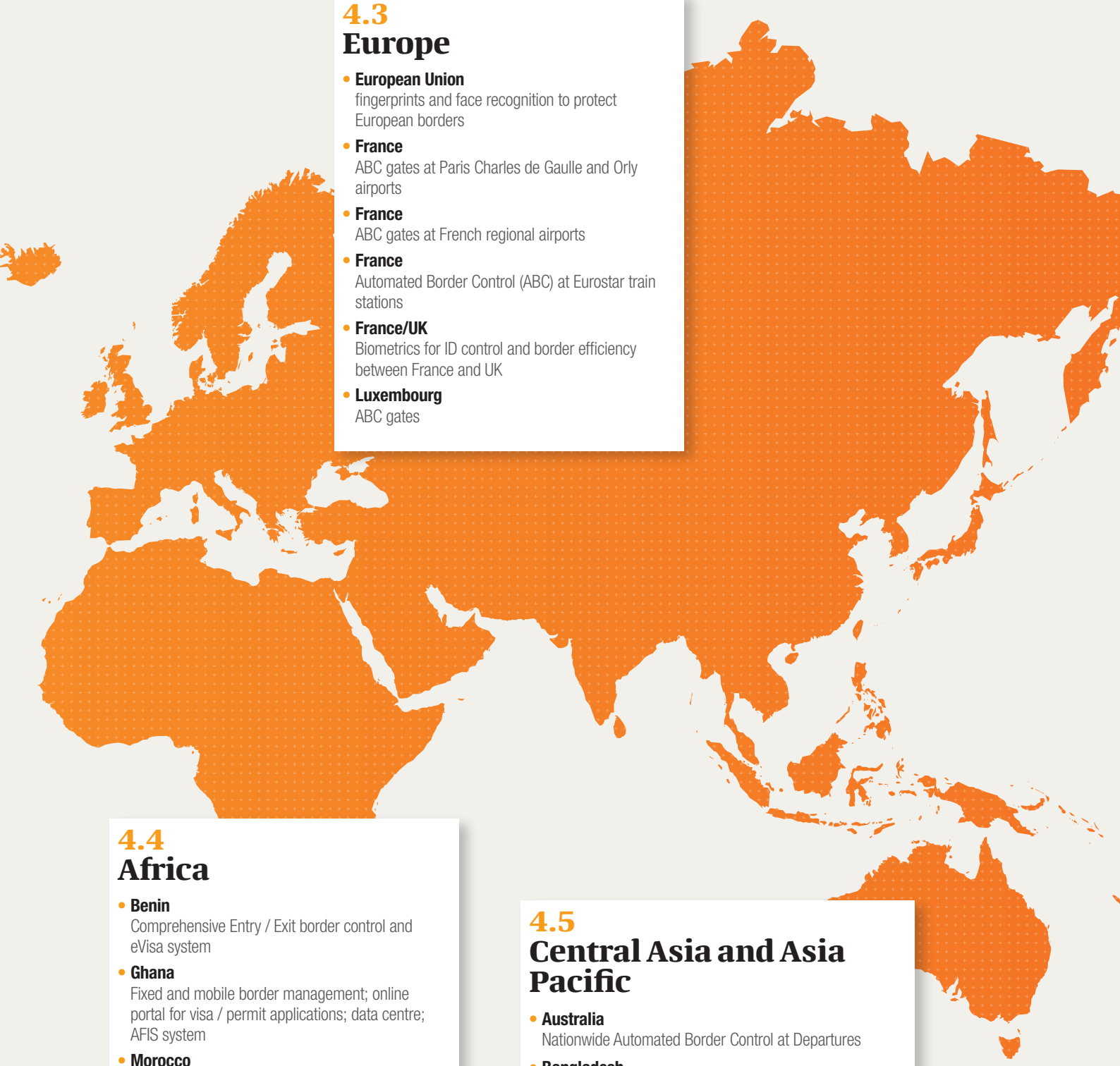
4. Case Studies

4.1 North America

- **Canada**
  Next Generation Cross-Border eGate Programme… NEXUS
- **USA**
  Biometrics at the border… US-VISIT
- **USA**
  Expediting passengers through the customs and passenger re-entry process

4.2 Latin America

- **Argentina**
  API / PNR, Traveller Analytics Suite (TAS)
- **Chile**
  border solution including API / PNR
- **Colombia**
  eGates with IRIS authentication
- **Honduras**
  Border Management System
- **Uruguay**
  Integrated Entry/Exit Border Management, etc.



4.3 Europe

- **European Union**
  fingerprints and face recognition to protect European borders
- **France**
  ABC gates at Paris Charles de Gaulle and Orly airports
- **France**
  ABC gates at French regional airports
- **France**
  Automated Border Control (ABC) at Eurostar train stations
- **France/UK**
  Biometrics for ID control and border efficiency between France and UK
- **Luxembourg**
  ABC gates

4.4 Africa

- **Benin**
  Comprehensive Entry / Exit border control and eVisa system
- **Ghana**
  Fixed and mobile border management; online portal for visa / permit applications; data centre; AFIS system
- **Morocco**
  Modern Border Control
- **Rwanda**
  Land border biometric border control with Congo, with eGates
- **Uganda**
  Visa management + BMS pre-check kiosks

4.5 Central Asia and Asia Pacific

- **Australia**
  Nationwide Automated Border Control at Departures
- **Bangladesh**
  End-to-end border control + ePassport system
- **Myanmar**
  Border control
- **Singapore**
  Changi International Airport
- **Tajikistan**
  Border Management + visa management system
- **Uzbekistan**
  Border control, biometric enrolment and online portal

Canada:

NEXUS Cross-Border RTP eGate program

Customer
Winnipeg Airport – CBSA (Canada Border Services Agency)

Opportunity/issue to address
Introduce Automated Border Control eGates for the NEXUS RTP cross-border programme between Canada, US, and Mexico at Winnipeg International Airport to alleviate the airport terminal and minimise contact-based interactions.

Solution
In September 2020, Winnipeg International Airport (Canada), in collaboration with CBSA, has introduced for the first time a bank of five Automated Border Control eGates for US/MEX entry travellers to cross the border making use of facial recognition to expedite immigration procedures.

Key components
- 5 x ABC eGates single door
- 1 x Orchestra™ Identity Management Platform integrated with CBSA NEXUS platform
- Facial recognition 1:1 and 1:N, passenger flow management and privacy-by-design
- NEXUS RTP Enrolment integrated with Border Management

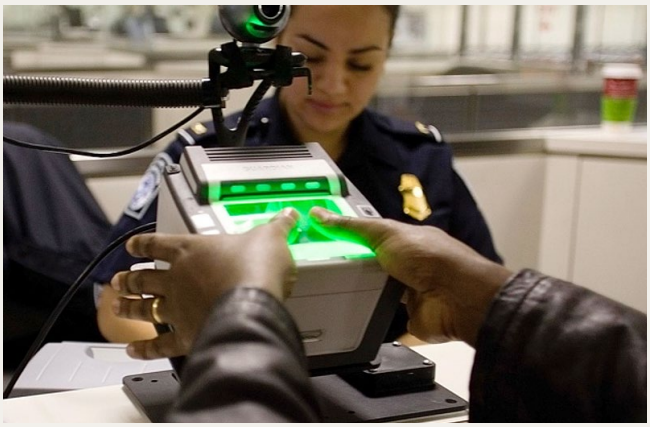
Customer benefits
- Simplify immigration procedures while improving ease, speed, and convenience for end users with biometric enrolment and automated process at the border in a full self-service approach, crossing the border in less than 10 seconds.
- All NEXUS users are eligible, thus enabling touchless travel at the border for greater security and safety in a post-COVID world, while increasing identity control accuracy.

Traveller benefits
- Passengers can cross the border in less than 10 seconds using their face as a token and enter Canada through their NEXUS membership instead of going to manual counters or using previously deployed NEXUS kiosks which implied physical interaction.
- Fewer lines, faster entry, and increased satisfaction.

vision-box

USA:

Biometrics at the border… US-VISIT



US-VISIT demonstrates that practical solutions can be deployed to collect, verify, and search major collections of biometrics in support of border security.

- Large biometric solution–measured by numbers of passengers recorded, database size, search performance, number of locations where the system is used.
- Common reference system for US government.

Scale

- 200,000 fingerprint captures per day
- 30,000 simultaneous users
- 115 airports using the system
- System is used operationally for the border (230 locations in the US) and visa processing (211 locations, globally)

Benefits

- Demonstrates the technology works at this very large scale.
- Face + fingerprint record created for each visitor.

THALES

USA:

Expediting passengers through the customs and passenger re-entry process

An ocean-going version of U.S. Customs and Border Protection's (CBP) Biometric Exit programme, the "Sea Re-entry" used IDEMIA's MFACE solution to verify that individuals disembarking Royal Caribbean Cruise Line's (RCCL) ships are the same ticketed passengers who boarded at the start of a cruise. An initial trial, conducted at Port Bayonne, N.J., demonstrated high-quality and high-speed facial matching.

- Facial recognition debarkation system using MFACE facial recognition devices, for debarkation
- Software configured to capture a passenger's face in real time and match it against the CBP Traveller Verification Service (TVS): 1:few match against TVS; installed at Port Bayonne, Port Miami (2), Port Everglades (3), Cape Liberty, Cape Canaveral, Portland, Galveston

Customer benefits

- High-quality, high-speed facial matching and feedback.
- Biometric-based.
- Better manpower allocation: CBP staff are realigned to focus on more targeted enforcement activities.
- RCCL customer is now able to board the next cruise faster.

Traveller benefits

- Less waiting times; faster debarkation process.
- Improved passenger experience; biometrics as a friendlier, more secure approach to border crossings.

IDEMIA

Argentina:

A modern API and PNR data collection solution and services

Advance Passenger Information (API); Passenger Name Record (PNR)

The Dirección Nacional de Migraciones (DNM) is building upon the successful operations of IDEMIA's API project (in operation since March 2017) and PNR project (in operation since March 2018), allowing a complete service for API and PNR data collection, applied in the international air and maritime transport industry.

- Scale: 7M transactions / year (6M for API, 1M for PNR); 32 International airlines connected (5 for PNR)
- Key technology: IDEMIA Traveller Analytics Suite™ (TAS) data collection system, hosted and monitored by IDEMIA
- "Solution as a Service" for:
  - » API and PNR data collection for air passengers (entry and exit)
  - » API data collection for maritime (cruises) passengers (entry)
  - » Processing of API and PNR data conversion, making it available to DNM on a local infrastructure

Customer benefits

- Fast system deployment (6 months).
- Effective solution to optimise resources, prevent and combat cross-border crime.
- Customised solution to help the government of Argentina improve API & PNR data processing.
- Comprehensive data collection of booking information for flights and cruises to and from Argentina.
- Privacy by design and compliance with national and international law.

Government agency benefits

- Effective and modern tool boosting efforts in fighting organised crime and illegal immigration.
- Adaptable solution that takes into account end-users' changing needs.

IDEMIA

Chile:

A modern API and PNR data collection and analytics solution

Chile sought an innovative solution to bolster homeland security and fight against cross-border crime. Consequently, the "Ministerio del Interior y Seguridad Publica" of Chile launched a call for tenders in 2018. IDEMIA proposed to implement an API-PNR data collection and analysis services in record time. Chile Government approved the contract in April 2019 and the project went live in June 2019.

- IDEMIA (with its partner IAFIS) provides installation and airlines connection/certification, as well as data collect and analytics services.
- Aims:
  - » Strengthening the border and the internal security of the country
  - » Modernising and streamlining the control process of entry and departure of people, from and to national territory
- Key technology: IDEMIA Traveller Analytics Suite™ (ITAS) data collect & analysis system, hosted and monitored by IDEMIA.
- Processing of API & PNR data, making it available to the "Ministerio del Interior y Seguridad Publica" on a local infrastructure in its data centre in Santiago, Chile.
- Expected throughput: 15M passengers / year; 32 airlines connected.

Customer benefits

- Fast system implementation.
- Effective and modern solution to prevent and combat cross-border crime.
- Comprehensive data collection of booking information for flights to and from Chile.
- Adaptable solution that takes into account end-users' changing needs.
- Improved border security thanks to easy interfacing with international systems.

Traveller benefits

- Travelers can now experience a smoother border crossing process.
- Privacy by design and compliance with national and international laws.

IDEMIA

Colombia:

Immigration gates

Customer

Migración Colombia and local partner Incomelec

Opportunity/issue to address

To reduce congestion for Colombian citizens re-entering the country with self-service gates and iris authentication at Bogota's El Dorado International Airport.

Solution

In February 2018, Migración Colombia officially launched **BIOMIG** – ABC gates using iris biometry to authenticate passengers. Key components:

- 10 gates
- Iris biometry solution and gate software integration.
- Enrolment integrated with border.

Customer 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.

Traveller benefits

- Passengers enter their flight number, look at the camera, and are processed in less than 25 seconds.
- Fewer lines, faster re-entry, and increased satisfaction.

THALES

Honduras:

Border management system

Customer

Instituto Nacional de Migracion

Opportunity/issue to address

- Consistently record traveller biometrics upon entry and exit to enforce national security. Connection with private systems, such as hospitality and car rental, to follow travellers during their stay in the country.
- Delivered and in capacity building phase.

Key components

- Thales Full Page ePassport readers for the airports along with biometric devices (102 desktop FP scanners and mobile devices).
- Implementation of border control stations at three main airports and 146 points of border crossings (land frontiers and sea ports).
- Development of a Thales Border Management Software Solution
- 1:N and 1:1 FRS (Thales Facial Recognition Platform), data shared between Instituto Nacional de Migración de Honduras and the National Police of Honduras, with the purpose to help the police in crime investigations.
- Database size: 1.5M records (10 flats each).
- All interfaces connect with other government software and platforms.

Customer benefits

- Register and identify travellers upon entry, during their stay and upon exit.
- Speedy enrolment of all travellers' biometrics (4:4:2) and picture taken, in order to start building the database.
- Data collected in Honduras BMS is shared with INTERPOL.

Traveller benefits

- Faster immigration processing of travellers at borders.
- Parental control features for children traveling in and out of the country to prevent trafficking.

THALES

Uruguay:

Immigration eGates and seamless flow

Customer

Aeropuerto de Carrasco – Ministerio del Interior Uruguay

Opportunity/issue to address

Establish a fully automated border control process at immigration (entry/exit), enabling self-service biometric boarding for all carriers as a second step.

Solution

In mid-2017, Aeropuerto de Carrasco (Corporacíon Americas), in Montevideo Uruguay, introduced the EASY AIRPORT programme that is enabling manual and automated border control entry/exit positions to make use of facial recognition to expedite migration procedures. In 2019, it also enabled the One ID concept which makes it possible for enrolled passengers at borders to confirm their identity through facial recognition and board the plane.

Key components

- 8 x ABC eGates using facial recognition and fingerprints (fallback).
- 21 x manual counter enrolment units for facial and fingerprints.
- 16 x self-service biometric boarding eGates using facial recognition.
- 1 x Orchestra™ Identity Management Platform integrated with immigration backend and airport systems, equipped with a last generation ABIS.
- Facial recognition 1:1 and 1:N passenger flow management and privacy-by-design.
- Enrolment integrated with border and airport systems, seamless travel enabled.

Customer benefits

- Simplify immigration procedures while improving ease, speed, and convenience for end users with biometric enrolment and automated process at border and boarding, with greater control of the end-to-end process.
- All traveller nationalities are eligible, aged 12 and over, to utilise the airport border and boarding processes in a contactless manner.

Traveller benefits

- Passengers enter their flight number, look at the camera, and are processed in less than 25 seconds.
- Fewer lines, faster re-entry, and increased satisfaction.

vision-box

Europe:

European Union: using fingerprints and face recognition to better protect European borders

The Schengen area, a travel zone where 26 European countries have abolished their internal borders, is key to facilitate the free and unrestricted movement of people.

The use of the latest biometric technologies makes it possible to ensure the protection of the external border for the long term. Based on European biometrics technology, this new system will first serve the identification needs of the new European Entry/Exit System (EES), thus being the cornerstone of the protection of European borders.

Along with Sopra-Steria, IDEMIA will develop the **shared Biometric Matching System (sBMS)** to serve the needs of the new **EES** and others. These systems will be operated by **eu-LISA**, the European Agency for the operational management of large-scale IT systems in the arena of freedom, security, and justice. The sBMS will be at the heart of the future EES as all Schengen Member States will use it to undertake the controls they have to perform at their border crossing points – land, air, sea and mobile.

Key features

- Designing and implementing the Biometric Matching System (BMS).
- Operational support: 24/7, corrective, adaptive, preventive, and predictive maintenance.
- Biometric knowledge.
- System stores the biometric information of short term Third Country Nationals (TCNs) when entering the Schengen area.
- Support identification of the TCN at a subsequent movement.
- Biometrics: fingerprints (4 flat), facial.
- Migration of the existing biometric system used at eu-LISA level (VIS, SIS, Eurodac) to the new sBMS.

Benefits for Schengen Member States and Europe

- Improved level of security.
- Integrated high-end and European biometric technology.
- An accurate, resilient, performant system for all member states.
- Gaining from the experience of consortium members who already support the European Union in the management of other mission-critical large-scale IT systems including VIS, SIS and Eurodac for more than 15 years.

IDEMIA

France:

ABC gates – Paris airports

Customer
Paris Aéroports

Location
Paris-Charles de Gaulle and Paris-Orly Airports, covering 52% of total air traffic in France with 100 M pax since 2017.

Opportunity/issue to address
Reconcile security and speed, cost-efficiency and convenience. Second generation eGates.

Solution scope
ABC Gates for entry and exit with automated identity verification and passenger authentication:

- Delivery of ABC Gates Solution with more than 100 eGates in operation at Charles de-Gaulle and Paris Orly International Airports.
- The eGates feature liveness detection, live face capture and quality assessment, enabling passenger's identity verification.

Just like other European major airports, Paris Aéroports has adopted facial recognition, instead of fingerprint verification. There are three main drivers for Paris Aéroports replacing fingerprint with face biometrics for their new ABC gate:

- First, facial recognition enables the gates to open to almost half of all travellers flying in and out of Paris airports, compared to fingerprint recognition which allowed five times fewer travellers to use the gates.
- Second, from a traveller perspective, facial capture is much less intrusive than fingerprint capture and way simpler, as it requires hardly any effort or specific action. This makes facial a much more friendly technology and helps drive user acceptance.
- The third driver is of course speed and accuracy. The average processing time per passenger is reduced 2x with face compared to fingerprint and the possibility of an error is significantly diminished compared to when the traveller has to present the correct finger(s) to the scanner.

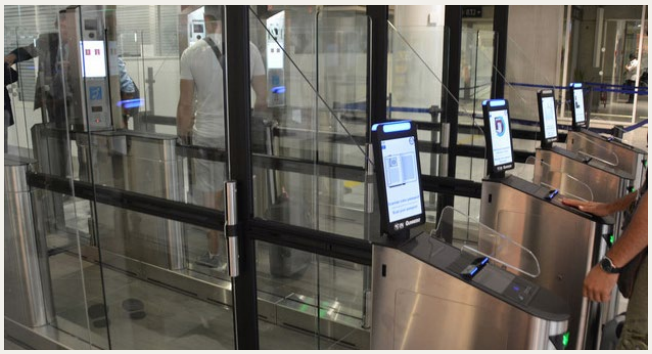
Production began in June 2017, with the gates being deployed progressively until June 2018, when migration to facial recognition started as requested by ADP.

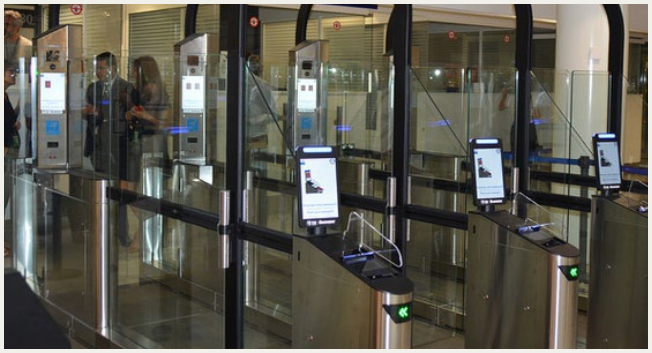
The last ABC Gates with fingerprint recognition were switched to facial recognition in December 2019.

THALES

France:

ABC Gates – French Regional Airports





Rationale

Cope with increasing **passenger numbers** and pave the way for further **automation at the border**:

- **Faster and more secure border crossing**: anti-spoofing, check number of persons, intrusion, etc.
- **Integrates into a global border control solution**: Mobile + Kiosk + eGate to start control in advance of arrival.

Large scale: In 2019, France had 90 M visitors arriving to the country. More than half arrived by plane.

Project

Deployment of ABC gates for Automated Border Control at four main French airports. The equipment allows eligible travelers to expedite their entry or exit to the Schengen area.

Benefits

- Paves the way for full automation.
- Proves the benefits of using biometrics and automation for border control.

France:

Automated border control at Eurostar stations

Customer

Eurostar and the French Ministry of the Interior

Opportunity/issue to address

Following a successful Vision-Box pilot at Roissy CDG T2 in 2016 to evaluate the introduction of facial recognition in the PARAFE Automated Border Control programme in France, and the subsequent publication of a ministerial decree authorising usage of facial recognition at the border, Eurostar has decided to introduce PARAFE III ABC eGates at both Saint Pancras (UK) and Gare du Nord (FR) train stations for EEU travellers.

Solution

In March 2017, Eurostar introduced several ABC eGates of the PARAFE generation III (facial recognition capable) at their UK and French train stations on behalf of the French Ministry of Interior and the DCPAF Border Police agency to expedite EEU travellers at French borders entry/exit. Travelers can use facial recognition, connected to the French government border control systems, to cross the border in less than 20 seconds.

Key components

- 8 x self-service biometric automated border control eGates at St-Pancras station.
- 5 x self-service biometric automated border control eGates at Gare du Nord station.
- 1 x Orchestra™ Identity Management Platform integrated with MOI DCPAF/DSIC Border Control systems.
- Facial recognition, passenger flow management and privacy-by-design.

Customer benefits

- Enhancing immigration procedures while improving ease, speed, and convenience for end users with self-service border control for expedited procedures for bona fide travellers, making it possible to process more than 1 million travellers per month.
- Starting at 18 years old, EEU travellers are eligible to use the eGates, thus enabling expedited Train on-boarding and Station exit at the border for greater security.

Traveller benefits

- Travellers can cross the border in less than 20 seconds using their face as a token.
- Fewer lines, faster crossing, and increased satisfaction.

vision-box

France / UK:

Biometrics for identity control and border efficiency between France and the UK

The border between France and the UK typically carries 2.6M cars, 21M passengers, and 1.6M goods vehicles.

IN Groupe and Eurotunnel are implementing the first large-scale land and sea border programme on this border to improve the fluidity of vehicle control. This solution is based on the use of biometrics to confirm the identity of people and perform quick and efficient border control without leaving the vehicle.

For this, different processes and adapted technical solutions are implemented according to the different types of vehicles (car, coaches, trucks). General principles rely on IN Groupe kiosk-based automated border control solution according to Entry Exit System (EES) that is expected to be operational in all Schengen countries by beginning of 2022.

This step allows vehicle passengers and driver to provide their travel ticket, travel ID, data, and biometrics (fingerprint and face) the first time they use the system.

- IN Groupe Identity Management Platform (IMP) ensures the correlation of the person's identity, its biometrics, travel ticket, in compliance with GDPR regulations. For people in the frequent driver programme who have given their consent for temporary storage of their information, they will no longer need to go through the kiosks during their next visits. The prior communication via the Internet or a mobile application, of passage information (ticket, license plate, names of people on board) will speed up the passage.
- The Eurotunnel control process carried out throughout the journey of the vehicle ensures that information is entered at the various points. A series of sensors (license plate, face photography, automatic counting of the number of people) enable information to be collected effectively and without impact on traffic and traffic time.

Once at the border control post, all validated biographical information is automatically communicated to the police. The control process is then very significantly accelerated, since it is a visual verification, all other controls having been carried out beforehand and masked time.

Benefits

- This new system and process will help border authorities to perform the extended border control imposed by the Brexit agreement, and prefigure EES controls, keeping the fluidity needed at the border in order to avoid congestion.

Luxembourg:

ABC Gates Smooth and secure border control in a modernised airport

Opportunity/issue to address

The re-design and modernisation of the border control gates were a crucial factor to ensure safety and efficiency, with fast handling and hassle-free processing, for both ground crew and passengers.

Key facts

- **2018** – launching of the gates at the airport
- **3.6M** passengers in 2017
- **10 gates** for automated border control

Benefits

- Infrastructure and design are easily adaptable and reusable.
- Site Acceptance Test (SAT) successfully passed in less than a year.

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

Benin:

Comprehensive entry/exit border control and eVisa system

With the rise of globalisation and the concomitant increase of passenger traffic in airports, today more countries face the risk of illegal border crossings than ever before. The Cotonou International Airport and the Beninese Ministry of the Interior needed to modernise their systems for controlling and registering entries/exists to and from the airport, and, more generally-speaking, to and from Benin's borders.

Key features

- Ten-year concession contract awarded by the Ministry of the Interior and Public Security of Benin on January 2017 to IDEMIA.
- Supply Cotonou airport with a biometric system and eCounters to control as well as register the entries and exits of all travellers.
- Deliver eVisa application process.
- Key technologies:
  - » MorphoWave (contactless fingerprint capture)
  - » TraveLane (eGate)
  - » eCounter
  - » eVisa application.

Customer benefits

- eVisa means less paper printing, which means lower costs for the government.
- Improved border control and security via greater anticipation of threats.

Traveller benefits

- More pleasurable experience of traveling.
- Travelers can apply and receive eVisa from the comfort of their own homes.

IDEMIA

Ghana:

Border and visa management system, including ABC Gates

Country profile

Among the world's top-ten fastest growing economies with 24 million inhabitants, 8+ million foreigners.

Opportunity/issue to address

Strong rise of immigration in the last five years (tourists and investors).

Solution scope

Border Management, Visa Management, AFIS, Interpol DB integration

- ABC gates: for secure and seamless passenger processing
- Case study: Ghana's e-Immigration Programme
- Ghana entrusted Thales with its e-Immigration system, which is central to the eGhana project – an ambitious plan to create a modern IT infrastructure that can support sustainable development in the years ahead.

Key components of the Ghana's E-immigration solution

- Fixed and mobile border management systems deployed in six main ports of entry.
- Digital visa and permit application processing and issuing.
- Implementation of an online portal for visa and permit requests.
- Datacentre and network upgrades.
- 10 Thales eGate systems for automated border control at Accra International Airport.
- A robust centralised Thales Automated Fingerprint Identification System (AFIS).

Customer benefits

- Border management systems will supply GIS with comprehensive information while checking the validity and integrity of travel documents.
- Expedited immigration processing of travellers at borders.
- Improved efficiency of citizen and foreign traveller services.
- Prevention of identity theft and fraud through biometric data capture.

Traveller benefits

- More efficient visa and permit processing with online application submission.
- eGate registration for citizens and frequent foreign travellers.

THALES

Morocco:

Modern border control

Fast passenger processing with additional security

The Kingdom of Morocco awarded Veridos the contract for designing and implementing a national border control system for land border posts, airports and sea ports. The contract also covers all IT infrastructure required for the project:

- 25 million travellers visited Morocco in 2019
- Equipping all relevant airports, sea ports and land border posts
- Border control via eGates takes just 14 seconds
- >1,200 workstations, 140 mobile kits, 2 data centres.

Project at a glance

- Ultra-modern border control system rolled out in less than a year.
- System covers all relevant land border posts, airports, and sea ports.
- Stationary equipment and eGates delivered to fixed border posts and mobile systems for border control at other locations.
- Enhanced performance and security in mandatory border control processes, such as standard primary inspection and in-depth check at a secondary inspection.
- Border control is linked to all necessary external systems.
- VISOTEC® Expert 600 passport readers and VISOCORE® Inspect.
- Central operational site, disaster recovery site, and regional servers set up.

Solution benefits

- Improved passenger flows as a result of faster border controls.
- Intuitive, easy, and speedy processing of arrivals and departures.
- Smooth harmonisation and integration of existing databases.
- More secure borders thanks to biometric scanning technology.
- Future-proof and flexible system able to adapt to changing needs.

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

Rwanda:

Land-border automated border control

Customer:
Directorate General of Immigration and Emigration

Opportunity/issue to address
The project was initiated to solve vexing problems that Rwanda's border agency, the DGIE, was dealing with at Poids Lourd on the border with Democratic Republic of Congo (RDC). These challenges included an inefficient manual screening process, long lines, forged travel documents, deficient data on border movements, among other issues.

Solution
In 2013, Vision-Box installed a set of 10 Automated Border Control eGates at the Rwandan Poids Lourd Border point with the Democratic Republic of Congo. The project, aptly named Automated Passenger Clearance System (APCS), secures, and facilitates the processing of 45,000 pre-enrolled citizens per day that cross the border for visits, business, and studies.

Key components
- 10 x ABC eGates + AFIS + Border Control Platform integrated with government systems.
- Fingerprints (upgrade to facial recognition in process), traveller flow management.

Customer benefits
- The APCS serves to augment the capacity of the border point by clearing on average 40 people in 1 minute, 2,400 in 1 hour, and 28,800 in a 12-hour span.
- To alleviate the stress imposed on border facilities and personnel, the APCS is designed to use a self-clearance process that reads the individual's enrolment card information and matches their fingerprint with the one enrolled in the system.
- Additionally, the capability and ability of border personnel is augmented by using biometric data to assure traveller identification, by issuing electronically verified border coupons, and integrating the APCS system with watch lists that communicate an alert in real-time in case of a hit.

Traveller benefits
- Cross-borders workers can now enter and exit Rwanda in a much faster and convenient manner, presenting strong identity credentials, despite the environmental challenges the land border represents.
- Fewer lines, faster exit and boarding, and increased satisfaction.

vision-box

Uganda:

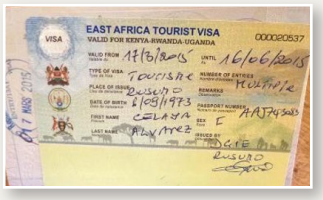
VISA management and BMS and pre-check kiosk

In July 2016, the Directorate of Citizenship and Immigration of Uganda selected Thales to enhance national security, protect the identity of travellers against theft, while offering an easy traveller experience. Support visa and work permit issuance. Thales started with the entire visa life cycle management from application to issuance. Online portal to apply and pay for eTA, visa management and issuance system at arrival to collect biometric data, check against control lists and AFIS.

In 2018 Thales delivered a full border control backend system with integrated kiosks for self-service at arrivals. Kiosks are deployed for the first step in the border crossing process. Travelers are eligible to use the kiosk, depending on their nationality and visa status. The solution captures and verifies the traveller's passport, captures travel data, captures and verifies a face picture, and captures and verifies four fingerprints.

Benefits

- Covers the whole visa lifecycle, from application to issuance



Visa issuance upon arrival after eTA check, verification of passports and collection of traveler biometric data

Centralised traveler database secured by an Automatic Fingerprint Identification System (AFIS)

THALES

Australia:

ABC smart gates at all departures

Customer

Home Affairs – Customs and Border Protection Services

Opportunity/issue to address

Australia's government, through its Seamless Traveller programme, aims to ultimately achieve 90% automation at the border (air/sea), through the usage of SmartGates and other biometric enabled solutions that will accelerate the adoption of contactless technology for all travellers.

Solution

In 2015 and 2016, Vision-Box installed 92 Automated Border Control eGates at all departures gates of international airports (10 sites) in Australia, using facial recognition.

Key components

- 92 x Next Generation ABC eGates + 1st and 2nd line border management GUI software.
- 1 x Orchestra™ Border Management suite with its operational and reporting tools.

Customer benefits

- Offer automated border control to the maximum number of departing passengers, regardless of their nationality or age (passengers must be a minimum of 1 meter high).
- To alleviate the stress imposed on border facilities and personnel, the system is designed to use a self-clearance process that reads the individual's traveller document information, authenticates it, and matches their face with the one from the ePassport chip or previously enrolled in the system at Arrival/Visa/Passport Office.
- Additionally, the capability and ability of border personnel is augmented by using biometric data to assure traveller identification and leverages a fully integrated second-line referral process by consuming data from the SmartGates.

Traveller benefits

- Passengers of all nationalities/ages can cross the border at Departures in less than 15 seconds, regardless of their travel document type.
- Fewer lines, faster exit, and increased satisfaction.

vision-box

Bangladesh:

End-to-end ePassport system and border control

Veridos has embarked on the broad-ranging modernisation of border control and passport production and introduced the first ePassport for the People's Republic of Bangladesh. The comprehensive project includes a state-of-the-art border control infrastructure and covers the entire value-chain for the creation of next generation ePassports, supported by modern, secure databases. The project is part of the country's mission and strategies for a Digital Bangladesh.

Project at a glance

- **Automated Border Control (ABC)** – installation of 50 state-of-the-art **eGates** at five sites.
- **Border control system** with manual control – improved passenger flows by faster processes.
- Introduction of an ICAO compliant electronic passports **(ePassports)** with a secure (and easy verifiable) high-definition colour image using CLIP® ID technology. Local production of 5 million documents / year.
- Introduction of Public Key Infrastructure **(PKI)** and Public Key Directory **(PKD)**.

Benefits

- Intuitive, easy, and fast processing of arrivals and departures.
- Secure borders due to biometric scanning and identity verification technology.
- Future-proof system adaptable to changing needs.
- Bangladeshi nationals holding the new ePassport can now use the new eGates on returning home to Bangladesh and will travel worldwide more easily and convenient relying on their new electronic passport.

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient and Bundesdruckerei

Myanmar:

Border control

Enhanced Border Control at the main entry points with a **Centralised View** and **Integration** to other systems:

- **Central entry/exit system** for supervision, reporting and data analysis.
- **Interfaces** to eVisa, watch list, others.
- **eGates, biometrics, card** for a Frequent Traveller Programme.

Context

- **4** international airports
- **16** border counters
- **4.4M** international visitors (2019)
- **Frequent Traveller Programme**

Benefits

- Enhanced security and control on Entry/Exit.
- Paving the way for border control automation.
- Integration to external sources of data and systems.

IN GROUPE

Singapore:

Changi International Airport, T4

Singapore's Changi International Airport is one of the busiest hubs in Asia. Getting passengers processed through passport control and onto their flights quickly and smoothly is a challenge in security, automation, user experience and technology. IDEMIA deployed cutting-edge biometric algorithms integrated in different passenger touch points to enhance the passenger experience for the opening of Changi Airport T4. These are now being rolled out across the airport.

Key figures

- 8M transactions / year after 1 year
- 300 passenger touch points
- 2017 project start

Project scope

- Automated departure management system (passenger processing system) integrates the whole departure process:
  - » bag drop
  - » airside access
  - » border crossing
  - » boarding.
- Exception management system: centralised and mobile.
- Interfaces with airport operational systems and government immigration systems.
- High availability: 24/7.

Customer benefits

- Faster processing of passengers allows for more time to enjoy the terminal facilities.
- Greater, non-intrusive security.
- Ability to re-deploy staff to customer service roles.
- Better optimisation of operating costs.
- EMS reduces turn-back queue disruption.
- Biometric partnership.

Traveller benefits

- Fewer touchpoints at departures – more pleasurable experience for traveling.
- Automated systems reduce language barriers and the need to provide multiple documents at multiple touchpoints.
- Travellers can arrive closer to flight time or get more work or leisure time in airline lounges – 10 minutes from check-in to board.

IDEMIA

Tajikistan:

Border management system and VISA management system

Customer

Ministry of Foreign Affairs

Opportunity/issue to address

Implement a biometric border control solution and an online and face-to-face visa management system for a facilitated visa application process to boost tourism.

Solution scope

Full Entry-Exit + visa management systems with HQ, disaster recovery and border management system.

In 2016 the ministry of Foreign affairs of the Republic of Tajikistan selected Thales to deliver a biometric Border Management System and an online Visa Management system to facilitate the visa application process and boost tourism.

The solution scope encompasses border and integrated visa management with Head Quarters. The border management system is deployed at 20 border points (including two international airport and land border points).

In 2019 the numbers of passenger at the border increased by 15% compared to 2018, thanks to the new border management system and the online visa application has shown a high increase too. This success is based on the security of the systems deployed by Thales.

THALES

Uzbekistan:

Border control

Aim

Improving both the **exchange of border crossing information** between ministries and the **border control for citizens and foreigners.**

Context

- Equipment of 71 border control points and interface with the border agency.
- **Biometric enrolment stations** (hardware and software).
- **Identity request management system** (AFIS IN Group and management of the secure issuing process) for 18 million citizens.

Benefits

- Provision of a reliable and efficient biometric identification system.
- An I/O control and management system providing the government with a complete, reliable, and efficient view of border control.

IN GROUPE

5. References

5.1 Organisations

Many organisations cooperate to make border security effective around the world, through local co-operation and via international or regional organisations. These include ICAO, IATA and ACI, INTERPOL, and European Union agencies.

INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO)

www.icao.int

ICAO is a UN specialised agency, established by the United States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).

ICAO works with the Convention's 191 Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable, and environmentally responsible civil aviation sector. In relation to border control, ICAO has published:

- **Traveller Identification Programme (ICAO TRIP)** is a strategy encouraging a holistic, coherent, co-ordinated approach to traveller identification management. This emphasis the dual aims of security and facilitation
- The **ICAO 9303** standard for Machine Readable Travel Documents (MRTDs), including the use of a secure electronic chip (microprocessor) to increase assurance about the document and its relationship to the person presenting it.
- ICAO maintains a global **Public Key Directory (PKD)** containing trusted public encryption key certificates essential to authenticating a secure document chip and its data.

You can view the ICAO Core Principles for Development of DTC (October 2020) here: https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guiding%20core%20principles%20for%20the%20development%20of%20a%20Digital%20Travel%20Credential%20%20%28DTC%29.PDF

INTERNATIONAL AIR TRAVEL ASSOCIATION (IATA)

www.iata.org

IATA is the trade association for the world's airlines. Its 265 members comprise 83% of total air traffic and IATA supports many areas of aviation activity and helps formulate industry policy on critical aviation issues.

AIRPORTS COUNCIL INTERNATIONAL (ACI)

www.aci.aero

ACI is the global trade representative of the worlds' airports.

OneID

https://www.iata.org/en/programs/passenger/one-id/

The **OneID** programme by IATA and ACI focuses on passenger facilitation, with close links to ICAO Digital Travel Credentials (DTC). IATA and ACI also run other related programmes, including **Smart Security** and **NEXTT**.

WORLD ECONOMIC FORUM

www.weforum.org

The World Economic Forum, committed to improving the state of the world, is the International Organisation for Public-Private Cooperation. The Forum engages the foremost political, business, and other leaders of society to shape global, regional and industry agendas. It is independent, impartial, and not tied to any special interests.

In February 2017, the Forum published **Digital Borders: Enabling a secure, seamless and personalised journey**. The report observed that the world is undergoing unprecedented change and called for a move from purely physical to digital borders integrated across the travel journey, from digital identification and authentication through biometrics to a frictionless airport transfer courtesy of digitally enabled security devices and the creation of a digital interface and individual profiles to increase accuracy, efficiency, and security.

You can review the publication here at: https://www.weforum.org/whitepapers/digital-borders-enabling-a-secure-seamless-and-personalized-journey

INTERPOL

www.interpol.int

INTERPOL enables police in 190 member countries to work together to fight international crime. INTERPOL provide a range of policing expertise and capabilities, supporting three primary crime programmes: counter-terrorism, cybercrime, and organised and emerging crime. In 2017 the Secretary General of INTERPOL, Jürgen Stock, called on passengers to encourage the responsible exchange of personal information including biometrics for advance visa entry clearance systems to make international travel safer and more secure. He quoted the 9/11 Commission Report: **"For terrorists, travel documents are as important as weapons."**

International travel features in many types of crime: people travelling to join terrorist groups in war zones; sex offenders travelling to foreign countries to commit offences; smugglers and traffickers (of goods and people) want to move between countries without their criminal purpose or real identity being discovered. Border security is therefore an essential part of tackling international crime.

INTERPOL's expertise and capability includes the Integrated Border Management Task Force (**IBMTF**), and the global Stolen and Lost Travel Documents (**SLTD**) database. INTERPOL's 27/7 global Command Co-ordination Centre (**CCC**) assists in intercepting many international fugitives, operating via each member country's National Central Bureau (**NCB**).

EUROPEAN UNION (EU)

The EU comprises 27 Member States (MSs) with a population of some 500 million. In addition, 26 member countries form the Schengen free travel area (including some that are not members of the EU). The European Commission is the executive of the European Union and promotes its general interest. Member states are responsible for their own border control and a number of EU agencies exist to help MSs do this, including EUROPOL, eu-LISA and FRONTEX.

EUROPOL

www.europol.europa.eu

Headquartered in The Hague, in the Netherlands, Europol assists member states of the European Union in their fight against serious international crime and terrorism. The agency also works with many non-EU partner states and international organisations.

Large-scale criminal and terrorist networks pose a significant threat to the internal security of the EU. Terrorism, cybercrime, and people smuggling, to name just a few, represent a severe threat to the safety and livelihood of its people. The biggest security threats come from terrorism, international drug trafficking and money laundering,

eu-LISA

www.eulisa.europa.eu

eu-LISA is the European Agency for the operational management of large-scale IT systems in the arena of freedom, security, and justice. The agency seeks continuously to add value to Member States' efforts for a safer Europe through:

- providing high-quality efficient services and solutions.
- building trust amongst all stakeholders, continuously aligning the capabilities of technology with the evolving needs of EU member states.
- growing as a centre of excellence.

eu-LISA operates a number of European-wide IT systems for law enforcement, including police information, visas, and asylum registration; and is also proposing systems to register visitors and to allow web-based travel authorisation.

EUROPEAN BORDERS AND COASTGUARD AGENCY (FRONTEX)

www.frontex.europa.eu

Frontex, the European Border and Coast Guard Agency, supports EU Member States and Schengen Associated Countries in managing the EU's external borders and fighting cross-border crime. With the newly created standing corps, Europe's first uniformed service, Frontex is present in the places where European countries need support, working together with them for a safer, more secure Europe.

5.2
SIA Initiatives, Tools and Publications

OSIA – Open Standards Identity APIs

https://secureidentityalliance.org/osia

OSIA is an interoperability framework for innovation, competition and sustainability.

OSIA is enabling governments to modernize, evolve and expand their foundational and sectoral ID systems so they can give every citizen access to a trusted legal identity and securely deliver a new generation of inclusive digital ID services.

Until recently, the initiation of highly functional and interoperable ID systems that are easy to upgrade or change has been constrained by a siloed approach leading to a lack of standardization that made it difficult to connect registries and exchange, consult, or update data between systems.

OSIA allows governments to be free to evolve, adapt, modernize, and add to their systems with confidence – without undue cost or time-consuming integration effort, and without fear of future compatibility issues.

In practice, OSIA is a set of Open Standards Identity APIs (interfaces) that makes it easy for governments to connect building blocks of their ID management system – independent of technology, architecture or vendor.

More information at: www.osia.io and https://github.com/SecureIdentityAlliance/osia

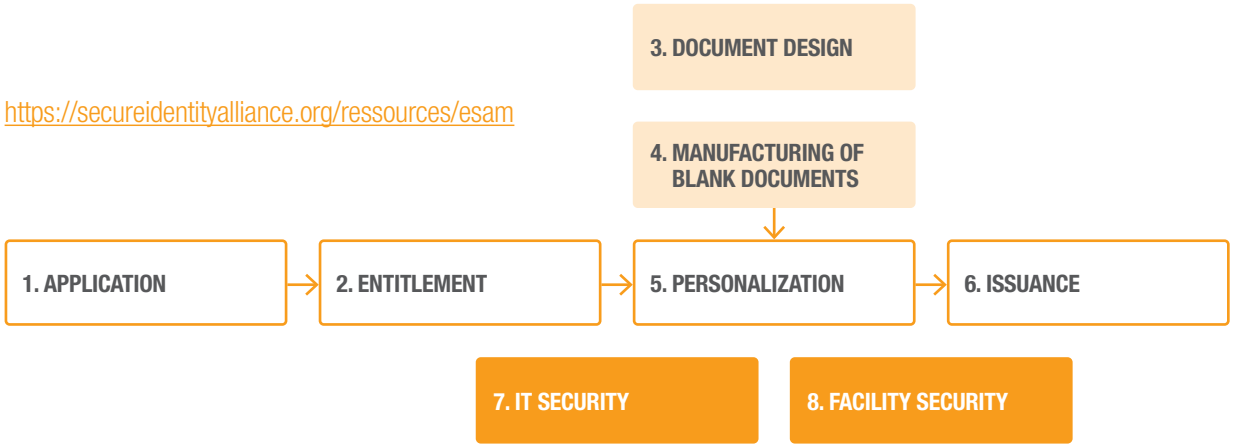
OSIA

eSAM – the eDocument Security Awareness Model

https://secureidentityalliance.org/sia-tools/esam

eSAM supports governments in the development of their eDocument issuance programmes – helping them understand what is required to build an effective 'security chain'. It can be used as a self-assessment tool to evaluate existing programmes, the security impact of additional changes, or to test multiple new scenarios. eSAM covers application, enrolment, document design, manufacture, personalisation, issuance, IT security and facility security.

https://secureidentityalliance.org/ressources/esam

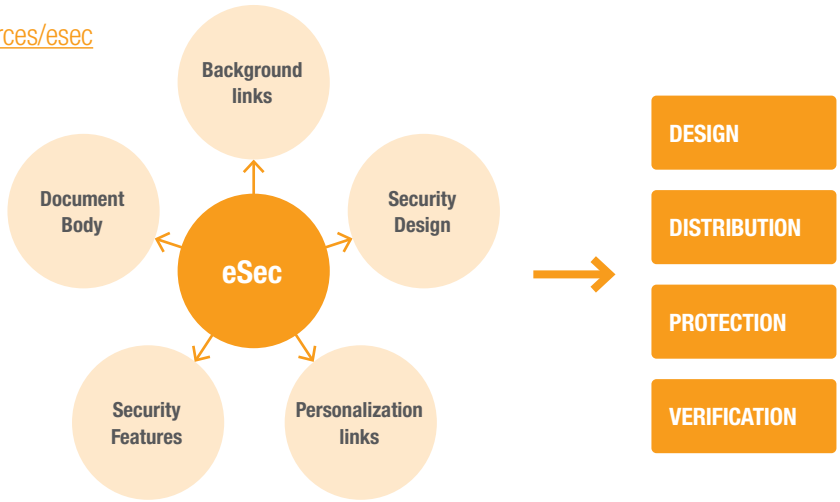


eSEC – the eDocument Physical Security Evaluation Model

https://secureidentityalliance.org/sia-tools/esec

eSEC is a self-assessment tool to evaluate the physical security features of your eDocument. eSEC covers security design, security features, document body, and the inks used for the background and for personalisation of the document; and how all of these features contribute to secure the design, distribution, protection, and verification of the document.

https://secureidentityalliance.org/ressources/esec



Other publications of the Secure Identity Alliance can be found at: https://secureidentityalliance.org/ressources/publications and https://secureidentityalliance.org/ressources/blog

5.3 Glossary

ABC	Automatic Border Control, for example, eGates
ACI	Airports Council International
ABIS	Automatic Biometric Identification System
AFIS	Automatic Fingerprint Identification System
API (1)	Advance Passenger Information
API (2)	Application Programme Interface
BMS	Biometric Management System (fingerprints, face and so forth)
BSI	German Federal IT Security Agency
DHS	Department of Homeland Security (US)
DTC	Digital Travel Credentials
EES	Entry Exit System (EU)
eSAM	eDocument Security Awareness Model (SIA)
eSEC	eDocument Physical Security Evaluation Model (SIA)
ESTA	Electronic System for Travel Authorisation (US)
eTA	Electronic Travel Authority
ETIAS	Electronic Travel Information and Authorisation System (US)
EU	European Union
eu-LISA	EU Agency for operational management of large-scale IT systems in the arena of Freedom, Security and Justice
EURODAC	Asylum registration system (EU)
FR	Facial Recognition
FRONTEX	European Borders and Coastline Agency (EU)
GDPR	General Data Protection Regulation (EU)
iAPI	Interactive Advance Passenger Information – can send a response when API is submitted
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICAO 9303	Standard for ePassports (MRTDs) and secure chips
MRTD	Machine Readable Travel Document – see ICAO 9303. eMRTD: including secure chip
OSIA	Open Standards Identity APIs (SIA)
PNR	Passenger Name Record
PKD	Public Key Directory – library of public key encryption certificates needed to allow secure chips and data to be authenticated
PKI	Public Key Infrastructure – complete infrastructure to support digital signatures being created and authenticated (see also PKD)
SIA	Secure Identity Alliance
SIS-II	Schengen Information System (EU) – law enforcement alerts system
SLTD	Stolen and Lost Travel Documents system (INTERPOL)
TRIP	ICAO strategy for border management
TVS	Traveller Verification System from US Customs and Border Protection (CBP)
US	United States
US-VISIT	System for traveller registration of entry to / exit from the US
VIS	Visa Information System (EU)
WHO	World Health Organization

Other reports by the Secure Identity Alliance:

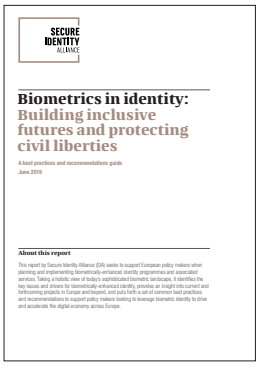
https://secureidentityalliance.org/ressources/publications

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.



Biometrics in identity: Building inclusive futures and protecting civil liberties

This report seeks to support policy makers when planning and implementing biometrically-enhanced identity programmes and associated services. Taking a holistic view of today's sophisticated biometric landscape, it identifies the key issues and drivers for biometrically-enhanced identity, provides an insight into current and forthcoming projects in Europe and beyond, and puts forth a set of common best practices and recommendations to support policy makers looking to leverage biometric identity to drive and accelerate the digital economy across the world.

SECURE
IDENTITY
ALLIANCE