eulisaroundtable.eu

Industry Roundtable
June 2022 - Report

Biometric Technologies in Identity Management and Verification

16 June 2022 | Strasbourg, France & online

eulisaroundtable.eu

eulisa.europa.eu

Catalogue number: EL-AN-22-001-EN-N
ISBN: 978-92-95227-05-7
ISSN: 2600-2728
doi:10.2857/647326

Table of Contents

Welcome and introduction

Krum Garkov, Executive Director, eu-LISA

In welcoming participants to the 15th roundtable, the Executive Director of eu-LISA, Mr Krum Garkov, emphasised the critical importance that these events have held since the Agency's establishment by fostering and facilitating **effective collaboration** that remains essential for delivering eu-LISA's mandate.

The EU' internal security domain is undergoing **significant transformation** as the management of external borders, internal security and migration are being integrated with the support of digital technologies. However, our challenges are not unique, and today we will hear from our colleagues in the USA Department of Homeland Security, particularly those responsible for customs and border protection.

Digital transformation is not only about deploying the newest technology, but mainly about changing the ways we use technology in the first place.

Thus, it is of paramount importance to regularly engage in such discussions, exchanging experiences and **identifying the best practices for utilising digital solutions** to support the ongoing transformation. In this regard, Mr Garkov stressed that digital transformation is not only about deploying the newest technology, but mainly about changing the ways we use technology in the first place. Therefore, it is essential to ensure the engagement and collaboration of **all stakeholders involved** – eu-LISA, the Member States, European Commission, other EU agencies, and the industry – to ensure the success of this ambitious project.

What is needed most today are not standalone technologies, but integrated end-to-end solutions that entail re-designed business processes and capacity building.

Mr Garkov continued his opening remarks by stating that what is needed most today are not standalone technologies, but integrated end-to-end solutions that entail re-designed business processes and capacity building. This is of critical importance, as it directly addresses Europe's political response to the **popular demand for more efficient and effective border management and stronger internal security.**

In closing, Mr Garkov stated that although this is the last Industry Roundtable under his leadership, **eu-LISA will continue expanding its role** as the facilitator of the dialogue between the EU Member States, Institutions and the industry, while also continuing to support the Member States and Institutions in keeping Europe safe and strong.

Welcome remark by the French Presidency of the Council of the EU

Jérôme Letier, Director of Digital Technologies Directorate, Ministry of the Interior, France

Mr Jérôme Letier welcomed the participants of the eu-LISA Industry Roundtable on behalf of the French government, currently presiding in the Council of the EU. He began his speech stating that the area of Freedom, Security and Justice embodies European values in that it guarantees the free movement of people, while also ensuring everyone's security in the exercise of fundamental freedoms that we all defend.

> *Technology offers a substantial opportunity for strengthening the capacity of internal security and border management authorities in making the EU a safer place.*

In this context, **eu-LISA plays an important role by spearheading the digitalisation of the Schengen area,** in particular through the development and operation of large-scale JHA IT systems, facilitating the exchange of information between Member States, which is **the foundation for the efficient functioning of the area of Freedom, Security and Justice.** As such, eu-LISA is the perfect example of the benefits of deepening European integration.

Mr Letier continued by stressing that technology offers a substantial opportunity for strengthening the capacity of internal security and border management authorities in making the EU a safer place. New technologies are constantly developed to combat terrorism, serious criminal offences, identity theft and fraud, and illegal immigration. However, close cooperation between the Member State authorities, EU Agencies and Institutions, and the industry is as critical as advances in technology. Public-private partnerships are essential for the development of novel technologies that address the ever-evolving needs of public authorities. In this respect, events such as the eu-LISA Industry Roundtable, are indispensable.

Continuing with his remarks, Mr Letier reiterated that our common objectives remain unchanged: to guarantee the internal security of EU citizens, and to secure the external borders of the Schengen area. In this task, we **depend on the large-scale JHA information systems overseen by eu-LISA,** and the Interoperability architecture, currently under development. However, with the evolution of technology and the tightening of the Interoperability timetable, the challenges we face keep increasing as well. In that sense, it is crucial that Member State authorities continue to adapt their digital instruments to the issues they keep encountering during the different phases of implementing the EU's JHA information systems. **We are all in this together** and we need to make sure that we tackle the issues as they emerge. Otherwise, we will not be able to reach our goals. Since biometrics are an essential part of the JHA information systems and related processes, ensuring the collection of high quality data is paramount.

As many other Member States, France has been actively working on developing and testing new devices for capturing high-quality biometric data also in more challenging conditions. To that end, French authorities have been conducting a number of experiments in collaboration with industry partners, e.g. in collaboration between the French Forensic Police and Isorg, a French company specialising in organic and printed electronics devices for large-area photonics and image sensors (see presentation).

With this in mind, the focus of this edition of the eu-LISA Industry Roundtable is on biometric technologies and identity management. One of our major challenges today is to ensure that public authorities deploy the **most efficient technologies for identity management** at border crossing points and in enforcing internal security. This roundtable will facilitate the **meeting of public sector needs with the innovations, ideas and expertise offered by the industry,** all in the interest of securing our joint area of Freedom, Security and Justice. In concluding his remarks, Mr Letrier thanked all participants for their commitment to making Europe smarter, stronger and more secure.

> *Public-private partnerships are essential for the development of novel technologies that address the ever-evolving needs of public authorities.*

Session I

16 June 2022, Strasbourg (France) & online

Setting the Scene

Chairs:
Aleksandrs Cepilovs – Capability Building Officer, eu-LISA
Istvan Racz – Senior Information Technology Officer, eu-LISA

USA Department of Homeland Security, Office of Biometric Identity Management

Lisa MacDonald, Director of the Identity Capabilities Management Division

Ms MacDonald opened her presentation with an overview of the Office of Biometric Identity Management (OBIM) at the USA Department of Homeland Security (DHS). Biometric data are used across a wide range of areas within DHS, including immigration and border management, law enforcement, defence and intelligence, as well as credentialing.

On the biometric continuum, OBIM is not responsible for the capture/collection of biometric data nor for the decisions based on biometric data; instead, the Office covers other stages, including biometric matching, storing biometric data, sharing of data, as well as analysis. OBIM's core operations include:

- operation of multimodal **Automated Biometric Identification System (IDENT),**
- manual fingerprint examiner verification services (where automation is insufficient),
- coordination with data owners for maximum information sharing.

IDENT, whose operation is overseen by OBIM's **Biometric Support Center (BSC),** is the national biometric matching system for rapid identification and verification used by DHS. The system contains searchable fingerprint records for more than 275 million identities. In pre-COVID times, IDENT processed more than 400 thousand searches per day for both foreign nationals and US citizens, including both criminal and non-criminal purposes. In addition to fingerprints, the system contains ca 1 billion facial images and ca 7 million pairs of iris images.

Business rules and filtering. IDENT provides services to more than 45 USA and international organisations. The BSC is staffed by trained biometric examiners and provides biometric verification and identification on a 24/7 basis in cases where the system is not conclusive, this includes: 10-print comparisons and verification, unknown deceased identification, latent comparisons, face comparisons and enrolments. OBIM operates in a **complex environment:**

- providing services to a large number of customers,
- hosing a diverse array of data,
- performing a wide variety of operations on the data depending on the customer it serves.

Therefore, the rules on what data can be collected and for what purpose, for how long it can be stored and with whom it can be shared, are extremely important. OBIM acts as data steward – when managing service requests it applies business rules and filters to ensure that only data that is relevant to the specific service request is processed. Similarly to the EU, the USA has enacted laws for the protection of personally identifiable information. In addition, OBIM applies DHS Fair Information Practice Principles, such as transparency, data minimisation, use limitation, purpose specification, data quality and integrity, security, etc.

Interoperability. Further on in her presentation, Ms MacDonald presented the approach to interoperability between the biometric systems operated by USA federal departments. Specifically, IDENT operated by DHS, **ABIS (Automatic Biometric Identification System)** operated by the USA **Department of Defence** (DOD), and the **Next Generation Identification (NGI)** system operated by the FBI under the USA Department of Justice.

In 2004, IDENT and IAFIS (predecessor of NGI) began sharing enforcement data to support secondary processing for USA Customs and Border Protection customer. In 2010, OBIM put in place a Rapid Response at air ports of entry for a combined response from NGI and IDENT to better support officers at the port of entry. In 2011, DHS signed an MoU on data sharing with the DoD. In the meantime, there was some semi-automated sharing of data for some of the DoD biometric-enabled watchlists. Mutual interoperability with the FBI NGI system was utilised.

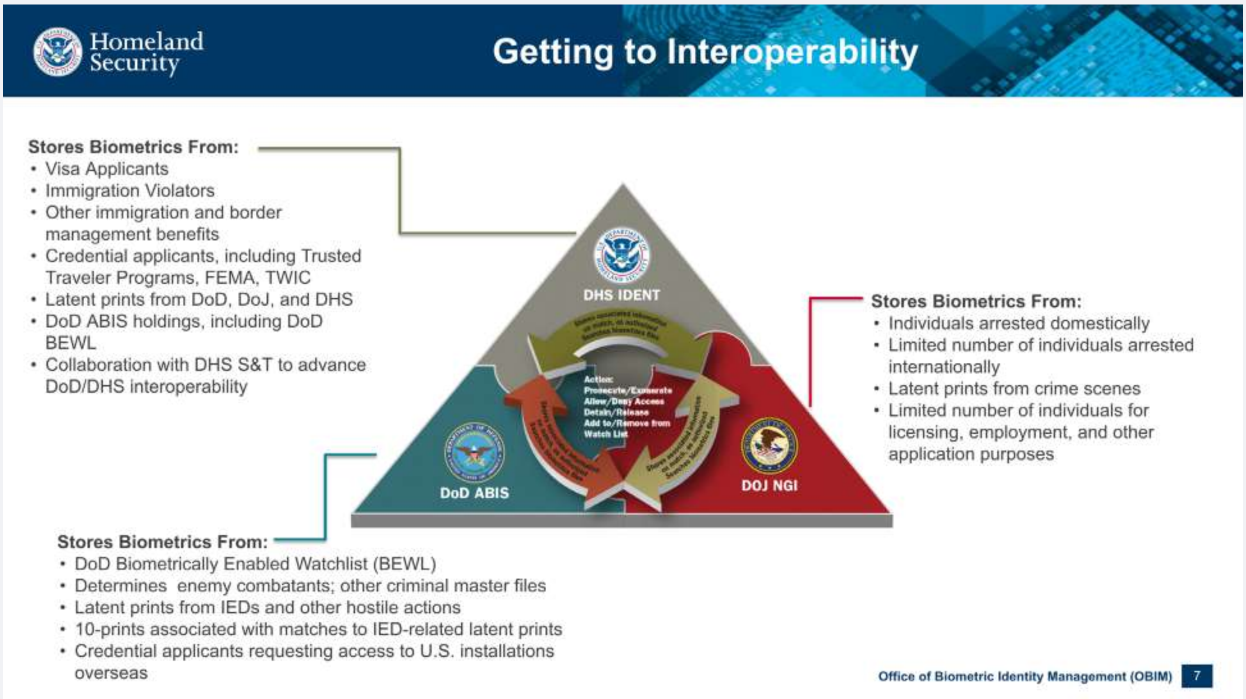
The **establishment of interoperability** between the three systems started with policy and legal framework, defining what data can be shared and under what circumstances. After a prolonged period of setting up

Keep an eye on the big picture! The technology is the engine that makes it go, but what is the vision? What are the business purposes you are trying to enable with biometrics, and how does the technology support that?

the legal framework, work began on interconnecting these independently developed systems that were using different message specifications, and data elements. Other major challenges were related to timing and resources, as availability was not necessarily matched at the same time across all organisations. Ultimately, systems interoperability enabled **more effective and efficient operation** on the frontlines.

Transitioning from IDENT to HART. In closing her presentation, Ms MacDonald provided an overview of the new system that is being developed by OBIM to replace IDENT, which has been in place since 1994 and is hardware-centric. The new system is called the **Homeland Advanced RecognitionTechnology (HART),** and it will provide new capabilities; expand interoperability with other systems; increase privacy and IT security; enhance accuracy; increase capacity, performance and availability; as well as improve cost effectiveness. The HART system will be hosted in a Federal Risk and Authorisation Management Program certified commercial cloud.

Looking ahead, OBIM will be expanding its multimodal collection and use of fusion; exploring other ways to provide identity assurance and accuracy; looking at additional modalities, taking into account the requirements inscribed in the legal framework; further improvement of algorithms (HART will introduce a marketplace for algorithms which will allow to test different algorithms and select on the basis of their performance); continue work on the development of standards; continue work on improving speed and throughput; and continue to look for ways to expand partnerships with different stakeholders.



Digitalisation of Travel Documents and Travel Facilitation

Mikko Hakkarainen, Policy Officer, DG HOME, European Commission

Mr Hakkarainen's presentation focused on the digitalisation of travel documents at EU level (incl. Member State pilot projects), and the Commission's ambitions in this area, the way forward with the implementation of the ICAO Digital Travel Credential (DTC), concluding with an overview how these elements complement the overall policy objectives of streamlining operations within the Schengen area.

EU approach to digitalising travel documents. Mr Hakkarainen stressed that when it comes to digitalisation, it is not an objective in itself or a panacea to all challenges we face, it is simply one of the tools for addressing a myriad of threats and challenges. Moreover, it is possible to digitise processes and services in full respect of fundamental privacy rights.

Digitalisation and AI can contribute to border management, identity and travel in several ways, e.g.:

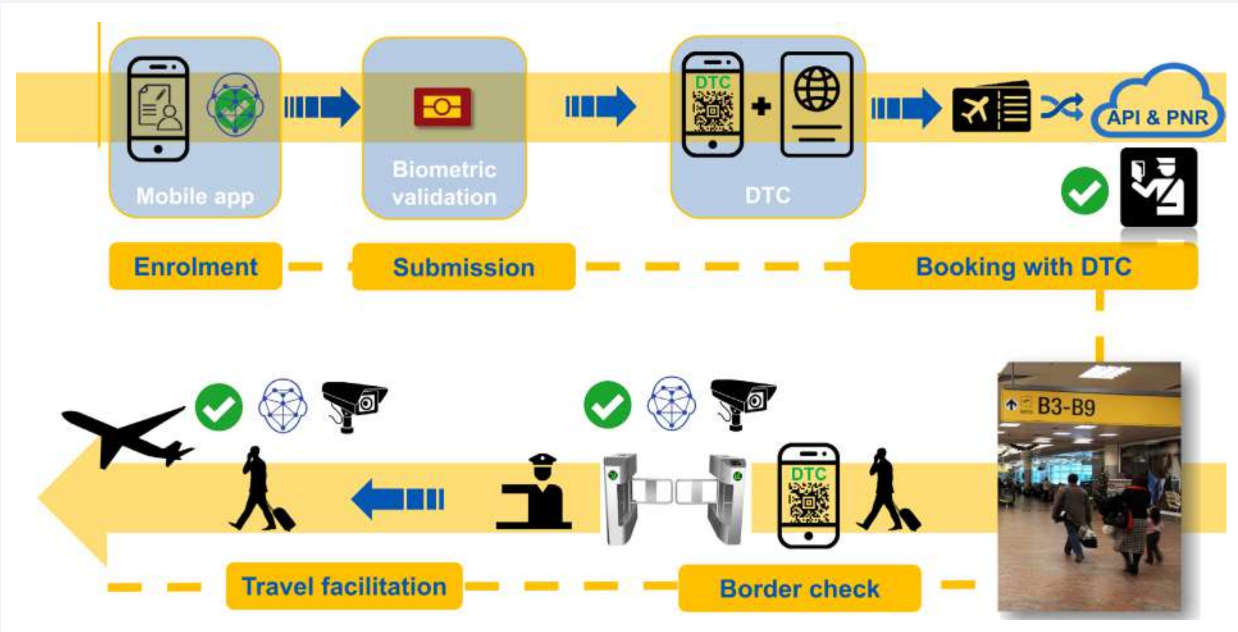
- border checks with systems that communicate with one another,
- verifying the authenticity of travel documents and compliance with the entry requirements,
- accelerating the overall process of border checks,
- and streamlining the whole travel experience for individuals.

In the **Schengen Strategy,** adopted in June 2021, the Commission committed itself to presenting, in 2023, a legislative proposal on the digitalisation of travel documents and facilitation of travel. This is not a standalone initiative, as the digitalisation of EU border management has been ongoing for a long time, including:

- digitalisation of visa procedure: making the application process and the visa sticker all digitalised,
- JHA information systems, notably SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN,
- support tools for operational users that do not contain any personal data, e.g. the False and Authentic Documents Online repository, which border guards can consult to see samples of almost all travel documents from around the world.

As such, it serves as the overarching framework for digital travel documents in the EU.

European pilot project on digital travel documents. Continuing his presentation, Mr Hakkarainen presented a pilot project on the digitalisation of travel documents, which will be carried out in collaboration with the Netherlands, Finland and Croatia. The project will test the creation, submission and inspection of digital travel documents, and identity verification at the border, culminating with the evaluation of their effectiveness, efficiency and security. The findings of this project will feed into the impact assessment in advance of a legislative proposal by formulating a proof of concept, and exploring the legal, economic, security and other impacts of using digital travel documents at the EU level.



The project will be based on the **ICAO Digital Travel Credential (DTC) specification,** and its Type 1 standard, an already existing international standard, easy to work with, important to ensure future global compatibility. However, all passengers would still be required to also carry a physical passport booklet.

Additionally, Mr Hakkarainen also presented an overview of the process encompassing all steps from the creation of the DTC to border crossing and travel facilitation.

The pilot project will support the legislative process by feeding into the impact assessment, achieving proof of concept and exploring the legal, economic, security and other impacts of digitalising travel documents at EU level and facilitating travel.

Privacy and data protection. Continuing his presentation, Mr Hakkarainen outlined some privacy and data protection considerations in the context of using DTCs, pointing out that these terms are often used interchangeably, although there is an important distinction between the two privacy right concepts.

Data protection right has evolved from the right to privacy, and both are aimed at protecting individuals from unlawful and unnecessary government surveillance. The distinction between the two is as follows:

- the **right to privacy** is a negative or a passive right, i.e. people should be **free from interference,**
- the **right to the protection of personal data** is a positive or active right, entailing a **system of safeguards, checks and balances** to protect personal data.

Both rights are also enshrined and guaranteed at the EU level, in the **EU Charter of Fundamental Rights.** These rights are relevant both in the case of the pilot project as well as upcoming legislation because authorities and service providers in the travel continuum will need to process different types of personal data, e.g. selling airline ticket, identity verification, conducting security checks, boarding the plane, etc.

Biometrics and facial recognition. Mr Hakkarainen emphasised that the processing of personal data will become even more sensitive once biometrics, i.e. facial images or fingerprints, enter the scene, and there are two main reasons:

- **legal considerations:** the EU's General Data Protection Regulation (GDPR) designates biometric data as belonging to the so-called special categories of personal data, whose processing is generally prohibited. Naturally, there are exceptions to this general prohibition, e.g. consent, reasons of substantial public interest;
- **public perception:** on the one hand, people have doubts as to the goodwill of governments in handling their sensitive information, on the other hand, people are sharing personal stories and pictures on social media.

The deployment of facial recognition technology in border management can provide security benefits, and allow individual travellers to cross borders without breaking stride. However, facial recognition constitutes a significant interference with the right to privacy and data protection. At the same time, public perception is also important – if we're not clear about the precise purposes for using facial recognition and how it is used, public trust is compromised, and the whole project could suffer.

While the use of **biometrics and facial recognition** in this pilot are proportionate, the interference with fundamental rights can be minimised, for example, with the following **safeguards:**

- limiting the data retention period to a minimum, e.g. only hours in pilot project, not days or years,
- using end-to-end encryption in all correspondence,
- implementing security measures to counter identity fraud and theft,
- clear rules on further data processing, ensure data accuracy to limit the amount of false negatives and positives, etc.,
- the best safeguard is to request the consent of data subjects, as in the pilot project.

Upcoming legislative proposal. All these implications for privacy and data protection will need to be assessed in the framework of the pilot project and as part of the overall impact assessment, and if all goes well, the European Commission will present a legislative proposal for the DTC in 2023, making the EU the first or among the very few early adopters of the digital passport in the context of international travel.

Identity Management at eu-LISA

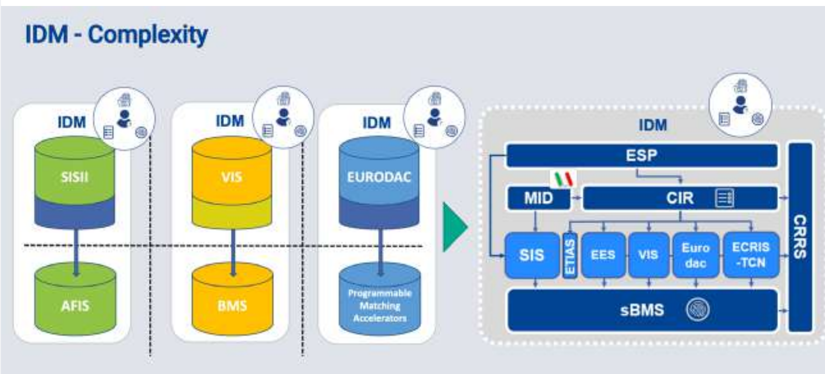
Istvan Racz, Senior Information Technology Officer, eu-LISA

Mr Istvan Racz provided an overview of eu-LISA' identity management (IDM) process, covering the existing legacy systems, and the new systems that will enter into operation in the coming years. The Agency's **identity management framework** includes:

- processes for creating, updating, and removing the identity of an individual,
- processes for verifying identities or identifying individuals,
- policies, technologies, and access rights and security measures.

In the context of the EU's JHA information systems, there are three different dimension to an identity:

- **biographical or alphanumeric identity data** (surname, first name, date of birth)
- **biometric identity data,**
- **associated business data,** i.e. visas, passports, identity cards, travel file information, asylum requests, alerts, etc., in line with the business requirements of specific systems.



Legacy systems. The Agency's legacy systems – SIS, VIS, and Eurodac – include different kinds of identity data. Currently, identity management is handled individually per system, with each of the systems operating within the scope of requirements defined by their respective regulations. However, this is changing due to the **Interoperability Regulation,** which entered into force in 2018, the purpose of which is fourfold:

1. to ensure that end users (i.e. border control, visas, asylum, law enforcement, etc.) enjoy fast, seamless, systematic and controlled access to relevant information,
2. to detect multiple identities and potential identity fraud across all JHA information systems,
3. to facilitate identity checks of third-country nationals,
4. to facilitate and streamline access by law enforcement authorities to non-law enforcement information systems at EU level.

Interoperability architecture. Implementing the Interoperability Regulation requires a fundamentally different technical approach to identity management – moving from the existing silo-based architecture to a more integrated approach. Identity management is supported by four strictly regulated components:

1. **European search portal (ESP),** single window for simultaneous queries,
2. **common identity repository (CIR),** a repository for all identity data stored across systems,
3. **multiple-identity detector (MID),** to combat potential identity fraud,
4. **shared biometric matching service (sBMS),** a gallery for biometric identifiers stored in the systems, allowing for synchronous and asynchronous queries.

There is one exception with regard to the legacy systems, namely identity data contained in the SIS will not be transferred into the CIR due to the specifics of the law enforcement domain and the requirements inscribed in the regulations. Instead, the SIS will connect directly to the sBMS.

The main purpose of the MID is to detect identities belonging to the same persons. The MID will identify similarities between different identities stored in the JHA systems, and decide whether two different identities might belong to the same person or not.

IDM – core requirements. The de-duplication process within eu-LISA's core business systems (CBS) will stay at the level of CBS, meaning that if a CBS doesn't allow for multiple identities to be stored for the same person, the CBS will apply the de-duplication process. In order to identify possible multiple identities, MID will perform two concurrent searches:

1. the **alphanumeric search,** and
2. a **biometric search**.

As a result of this operation the system will make a decision if these identities belong to the same or different persons. If the system detects multiple identities belonging to the same person, this outcome will be reviewed by a human examiner. MID will create Yellow and White links automatically, which will be further re-categorised by human examiners into Green (different persons) or Red (confirmed suspicion of identity fraud) links.

Implementing the Interoperability Regulation requires a fundamentally different technical approach to identity management – moving from the existing silo-based architecture to a more integrated approach.

To sum up, the Agency's identity management requirements include:

- accuracy of the sBMS and CIR, and also of manual processing when establishing links,
- data quality: quality requirements for biometric and biographic data are critical in ensuring the accuracy of IDM services,
- throughput and performance, including different priorities for business use cases,
- security and data protection, i.e. ensuring data integrity, privacy and confidentiality.

IDM – complexity. In the context of the Interoperability architecture, the complexity of identity management is extremely high, i.e. it is not enough for the individual components to perform well, the whole interconnected system needs to perform sufficiently.

IDM – key success factors. Concluding his presentation, Mr Racz outlined some of the key success factors for effective implementation of identity management, including:

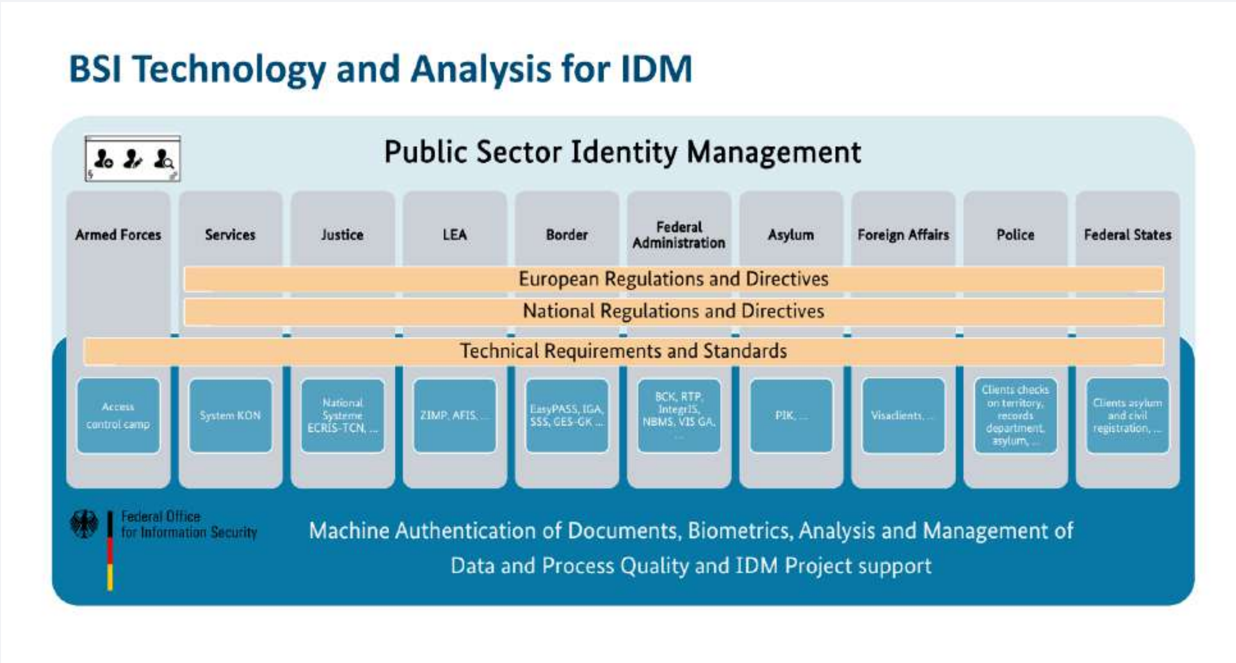
- rely on **standards** for defining protocols, data quality, containers, etc.,
- identity management needs to have a good **governance model** that brings together the expertise from different domains to find joint solutions,
- **innovations** in terms of approaches and technologies,
- further work on **biometric test data,** including on the potential to use synthetic data.

Biometric Identity Management in Germany

Markus Münzel, Federal Office for Information Security, Germany

Mr Münzel opened his presentation with a brief overview of how identity management is defined in the German public sector context. The German Federal Office for Information Security (BSI) provides an overall framework for identity management, including regulations and requirements, as well as technology. Hence, within BSI, identity management is understood as all IT-supported administrative measures enabling efficient and secure legal enrolment, update or verification of a person's identity.

Public sector stakeholders. BSI provides identity management services across a wide range of public sector stakeholders, including the Armed Forces, judicial and law enforcement authorities, border management, asylum and police authorities, as well as administrations at both federal and state levels.



The services provided by BSI include biometric matching services, data and process quality analysis and management, machine authentication of documents, as well as IDM project support.

More specifically, BSI offers the following **services to national agencies:**

- specification and standardisation for systems for document checks, biometric systems and identity management processes, including technical guidelines, certification and advice on demand,
- development of IDM solutions and Proof-of-Concepts for public sector identity management,
- technical and business analysis in operative systems.

In order to enable the data driven analysis, BSI runs a technical platform and infrastructure, which includes data science, data services and data engineering.

Standardised, efficient, and secure IDM processes. Mr Münzel continued his presentation with an overview of the **yellow link clearing process** within the context of interoperability. In order to clear a yellow link, we need to answer the following questions:

- what is the **biometric information** and its quality?
- what is the **alphanumeric information** and its quality?
- what is the **identity structure information**?

These questions need to be answered within the context of existing primary and secondary legislation, interface control documents, national legislation, and expert knowledge. To ensure this, BSI together with other agencies is working on the definition of a standardised, efficient and secure process for vetting or clearing the yellow links.

The other business side is the use of links. Here, the same information pertaining to biometric and alphanumeric data needs to be assessed; however, what is missing is a specification of best practice or guidelines on how to integrate this information into business processes.

Closing his presentation, Mr Münzel summarised that **identity management is the interplay between biometric, alphanumeric data and business processes,** and their analysis to enable efficient and secure business. We should remember that we build identity management solutions not as an end in itself, but to enable the business.

Identity management draws on expertise from different areas – biometrics, alphanumeric data, and business processes – to enable efficient and secure business operations.

Session II

16 June 2022, Strasbourg (France) & online

Biometric Solutions and Business Processes for Passenger Processing at Land/Sea BCPs: Industry Presentations

Chair:
Javier Galbally – Senior Capability Building Officer, eu-LISA

Proof of Concept – Mobile Fingerprint Scanner and Palm Scanner

Jennifer Aflalo, Biometry Security & Identity Program Manager at Isorg
Christoph Abraham, Head of Operational Engineering at the French Forensic Police

Mr Abraham kicked off the presentation by providing an overview of the context and the main motivation for the development of the proof of concept for a new mobile fingerprint scanner. Namely, the French Forensic Police had identified a **number of use-cases** where such mobile scanners could be used in place of traditional bulky fingerprint scanners **in daily field operations,** for example:

- **crime scene examinations.** Majority of the fingermarks (i.e., latent fingerprints) recovered from crime scenes do not belong to the perpetrators, but to bona fide subjects, e.g., people whose homes have been burgled. Mobile fingerprint scanners would allow excluding victim fingerprints, and narrowing down the search to the fingermarks of the criminals, significantly **expediting the investigation of crimes.**
- **identification of cadavers.** The ability to capture cadaver fingerprints in the field (e.g., at the scene of an aeroplane crash) would significantly **reduce the time required to identify the victims** by enabling immediate searches in fingerprint databases, without having to move the cadavers to the forensic laboratory, which can be a very time-consuming process.
- **verification of identity and right of residence.** During **routine on-the-spot checks,** mobile fingerprint scanners would allow law enforcement officers to conveniently verify the subject's identity, without having to relocate for fingerprinting purposes.
- **enrolment to information systems.** Currently, the enrolment of fingerprints to national IT systems can only be done at specific facilities, thereby **slowing down the investigation process.** Mobile fingerprint scanners would significantly expedite the process, for citizens and law enforcement alike.

Key functionalities. Based on these business use cases, the mobile fingerprint scanner was deemed to need the following key functionalities. First and foremost, **the device should operate autonomously,** without being physically connected to other pieces of equipment. In addition, it should be able to capture:

1. **both flat and rolled fingerprints,**
2. **single finger, and four finger impressions,** i.e., slap impressions,
3. **palm impressions.**

Proof of Concept project. Ms Aflalo, Biometry Security & Identity Program Manager at Isorg, continued the presentation with a brief overview of the company, which specialises in the manufacture of large image area sensors based on **Organic PhotoDiode (OPD) technology.** The OPD technology fit perfectly with the requirements specified for the mobile fingerprint sensor, leading to the two organisations to collaborate on the proof of concept.

In addition to the four requirements specified above, the partners decided to try for a common **smartphone size** (~120x60mm²), and defined a number of **technical quality criteria** for the scanner in order to comply with the FBI certification standard for fingerprint readers, e.g., False Acceptance Rate (FAR) / False Rejection Rate (FRR), resolutions, uniformity, and dynamic.

In the course of development, another key feature which was not included in the initial specifications, was added to the new scanner – the **ability to scan not only fingerprints but also paper documents,** e.g., ID documents, fingermarks recovered at a crime scene. Law enforcement officers found this additional functionality, coupled with the fingerprint sensor in one device, to be a great idea and very convenient.

Overall, the project produced altogether **three prototype evolutions,** with the last one showing equivalent performance to traditional FBI-certified scanners based on optical technology, i.e. prism scanners and light emitting scanners. Tests were conducted both on **image quality level** of the fingerprint samples produced, and on the accuracy in terms of FAR/FRR obtained when using those samples on the AFIS systems of the French Police.

Next steps. The project is **still ongoing**, with a view to adding the following elements:

1. improvement of module **robustness to bright sunlight,**
2. scanning function for **rolled fingerprints** (as per initial requirements),
3. **video function** to have direct feedback on fingerprint imaging and the quality of samples,
4. a more compact **module integration.**

LIVETOUCH Flipcase Mobile Identification Solution

Ondrej Adamek, Sales Manager at JENETRIC

Mr Adamek presented a new mobile fingerprint scanner developed by JENETRIC specifically designed for use at **challenging Border Crossing Points (BCPs),** e.g. land borders with limited resources and infrastructure that are not easily accessible, or sea borders with a high volume of travellers arriving in batches. In these scenarios, border guards need to manage a **great diversity of travellers** (i.e. nationals, tourists, workers, truck drivers, etc.) often with no pre-warning and arriving in various crossing modes (i.e. pedestrians, cars, buses, trucks, trains, ferries, etc.). In addition, in these BCPs it is not always possible to have fixed **kiosks for fingerprinting and identification of persons** as is the case for more controlled environments with well-equipped facilities, such as airports.

Compared to their heavy and bulky predecessors just a decade ago, modern fingerprint scanners have shrunk down to the size of a chocolate bar.

Evolution of Mobile Technology. A decade ago, mobile biometrics kits were heavy and bulky, and most importantly, non-autonomous, i.e. needing external power supplies and connection to a PC/laptop. The key enabler allowing JENETRIC to develop their **new smartphone-enabled solution** has been the evolution of mobile technology over the last decade, resulting in a new generation of smaller, lighter and more powerful devices with very high connectivity and computing capacity.

LIVETOUCH Flipcase. JENETRIC's newest device, combining a smartphone with a fingerprint scanner compliant with the **FBI-certified Fingerprint Acquisition Profile 60** (FAP60), is back-compatible with traditional fingerprinting scanners, and also with existing fingerprint databases. Additionally, the device is **compliant with the requirements set out by the eu-LISA EES Working Group** in their report for **ICT Solutions for External Borders** (sea/land), incl. the following operational and hardware specifications:

Operational requirements:

- battery-powered,
- easy and quick to set up and use,
- biometric data capture with the required level of quality,
- allowing freedom of movement while operating the device.

Hardware requirements:

- embedded camera with dedicated lighting capabilities, e.g. flashes,
- GPS to record the exact position of the border check operation,
- scanner to capture four flat fingerprints, i.e., slap impressions,
- flashlight function, e.g., to illuminate and read ID documents,
- screen privacy feature, i.e. display visible only to the operator.

The result is a new class of **compact and user-friendly** fingerprint scanners **designed for mobility** and multipurpose usage, with a significant simplification of the fingerprint capture process.

EES Register Tablet Solution Used in the Frontex EES Pilot

Cédric Lemonnier, Public Safety & Defense Project Manager at NTT DATA

NTT Data EMEAL project manager for Public Safety & Defense, Cedric Lemmonier, presented the **tablet solution developed for proof of concept testing in the Entry/Exit System (EES) pilot project** conducted by Frontex in 2021 at the Border Crossing Point (BCP) between La Linea de la Concepcion, Spain, and Gibraltar, UK.

FRONTEX EES pilot project. The main goal was to test new border-crossing solutions in a challenging **real-life operational environment,** specifically a **portable unit for seamless border crossing** for all types of travellers, both pedestrians or passengers sitting in a vehicle, while also **performing enrolment and identity verification of third country nationals (TCNs) in EES.**

Mr Lemonnier explained that **existing solutions** for this type of context involve a **time-consuming** process which can be cumbersome for travellers and border control agents, entailing:

1. **enrolment** of the TCN at a supervised fixed kiosk,
2. **verification** of the identity of the traveller, typically in a cumbersome biometric corridor or at a manned service desk,
3. **border crossing,** involving a border agent to double-check that the preceding enrolment and verification stages were successful.

For NTT, the main objective for the **all-in-one tablet solution for EES** was to try to simplify this process for both border guards and travellers by **speeding up the border-crossing time, while also reducing the amount of equipment and human resources required.** The tested tablet solution, operated by a border control agent and boosted with 4G, WiFi and Bluetooth connectivity, allows for the following two workflows for TCNs:

1. **first-time enrolment in the EES,** includes the following steps:

- reading and verification of travel document (passport) data (MRZ and chip),
- running an automatic search in national system linked to EES,
- live facial image capture and verification against the picture stored on the passport chip,
- live digital fingerprint capture and quality check,
- sending biometric and alphanumeric data for registration in the EES;

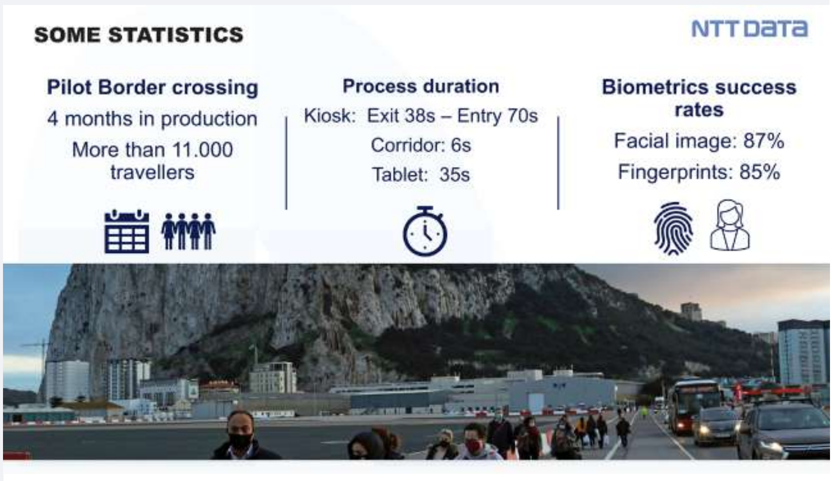
A novel all-in-one tablet solution, tested in real life environment, adaptable to different border-crossing scenarios involving pedestrians and passengers seated in vehicle.

and

2. **verification of returning TCNs in the EES:**

- reading and verification of travel document (passport) data (MRZ and chip),
- running an automatic search in national system linked to EES,
- displaying traveller file and travel history registered in EES.

Mr Lemonnier concluded the presentation by sharing some performance indicators. Overall, the test involved more than 11 000 travellers over a time-span of 4 months, and demonstrated a **significant reduction of the border-crossing time, especially for TCNs** traveling to the EU for the first time, and required to enrol in EES.



Evaluation and improvement of eu-LISA Synthetic Biometric Datasets

Marcel Grimmer, Researcher and PhD Candidate at the NTNU Biometrics Laboratory

The presentation focused on the joint project between eu-LISA and a consortium of partners involving the Norwegian Biometrics Laboratory at the Norwegian University of Science and Technology (NTNU) for the generation and analysis of synthetic facial biometric data.

Project overview. The project was motivated by eu-LISA's need to **train and evaluate its biometric-based recognition algorithms** using large datasets of biometric samples. Since using real biometric data for such purposes is prohibited by data protection regulations, the Agency teamed up with the team of researchers to explore possibilities for **substituting real biometric data with synthetically generated samples** in the training and evaluation of biometric systems.

Although the overall project scope was much larger, encompassing the analysis of different sources of variability in both real and synthetic face images, e.g. head pose, facial expression, and illumination, the presentation delivered by Mr Grimmer focused on **the problem of ageing in face recognition.**

Experimental Setup. The purpose of the experiments was to **determine whether synthetically aged facial images behave in a similar fashion to real face samples with the passing of time,** when analysed and processed by automatic recognition systems. To that end, both real and synthetic data were analysed from two perspectives: **quality and accuracy,** i.e., mated and non-mated score distributions.

GAN-based algorithms. Synthetically aged data was produced using Generative Adversarial Networks or GAN-based algorithms, a revolutionary technology that has dramatically changed the landscape of artificial face generation. The first pioneering study using convolutional GAN technology was published in 2015, presenting very promising results, but the artificial faces were easily distinguishable due to various visible artefacts. During the past 5 years, this AI-based technology has evolved greatly, and the current generation of GANs are capable of producing synthetic images that are almost impossible to discern from real facial pictures, offering multiple potential applications in biometrics, including:

- evaluation of the impact of face ageing on Face Recognition Systems (FRS),
- training of algorithms to increase the robustness of face recognition systems to the ageing effect,
- reduction of false negative identification rate (FNIR) by compensating the age gap between probe and reference samples.

Face age modification (FAM) experiments. The NTNU researchers produced synthetic databases using generative models to predict two things:

1. **future appearance (ageing),** and
2. **past appearance (rejuvenation).**

The experimental protocol compared the behaviour of synthetic face images to the performance of real databases containing multiple samples of the same individual taken over longer periods of time, while reducing other non-age-related sources of variability (e.g. head pose or illumination) to the maximum extent possible. The results showed very similar characteristics between synthetic and real face images, both from a quality standpoint (i.e., using automated quality metrics), and an accuracy perspective (i.e., using well established automatic face comparators).

Conclusions. The presentation highlighted the following key takeaways:

1. further experiments recommended to evaluate the robustness of face recognition systems in applications with long-term age differences between reference and probe image,
2. further testing of synthetically produced data still required, including more reliable quality metrics and a greater diversity of face comparators,
3. lastly, but most importantly, in spite of great progress, **synthetically generated face image data is still not ready to fully substitute real data for the training and evaluation of operational systems,** which still needs to be performed on real data (as stated by the ISO/IEC 19795-1: 2021 standard).

However, despite these reservations, synthetic data can be a very effective tool for, e.g.:

1. **system optimisation tests**, i.e. in terms of throughput,
2. as a complement in **performance assessment campaigns** carried out on real data in order to establish a first reliable estimation of system accuracy.

Enhancing Biometric Applications to Protect Privacy

Vincent Bouatou, Deputy Director for Strategic Innovations at IDEMIA

In closing the II session, Mr Vincent Bouatou, the Deputy Director of Strategic Innovation at IDEMIA, delivered a presentation providing valuable insights into the future of by-design privacy protection techniques for biometric applications. He set the scene by giving an overview of the main reasons that render **biometric systems highly sensitive**, which include their use

- in critical missions, such as border control, public security, or criminal investigations;
- for processing sensitive **personal data or personally identifiable information (PII) which is non-revocable,** i.e., if your fingerprint images/templates are compromised, it is not possible to issue new ones as with a PIN number or a security token.

Protecting personally identifiable information, and ensuring privacy requires an approach tailored to each specific use case.

The **highly sensitive nature of biometric systems** inevitably leads to the **mutual assurance of trust** between service providers and the users who are operating on the basis of two conflicting set of objectives:

1. users are interested accessing and using the service, with **minimal risk to PII,** e.g. leakage,
2. service providers are interested in correct user **identity verification,** while also adhering to compliance requirements.

Thus, **ensuring the necessary level of trust between both parties** is one of the major challenges faced by modern biometric solutions, which can be addressed by a **Trusted Third Party (TTP) via minimal disclosure systems enabled by biometrics.**

Building on these premises, Mr Bouatou went on to propose solutions that utilise newest technological developments and the most recent research to deliver an enhanced level of privacy protection and security – and, therefore, also trust – by-design in two most commonly used architectures utilising biometric technology:

1. **Centralised databases.** For example, in border management (e.g., the forthcoming Entry/Exit System), where a central authority stores the data of certain people and monitors their border-crossings. In this scenario, users (i.e., the person crossing the border) are asked to trust the service provider (i.e., central authority giving access to a territory) with their biometric data.

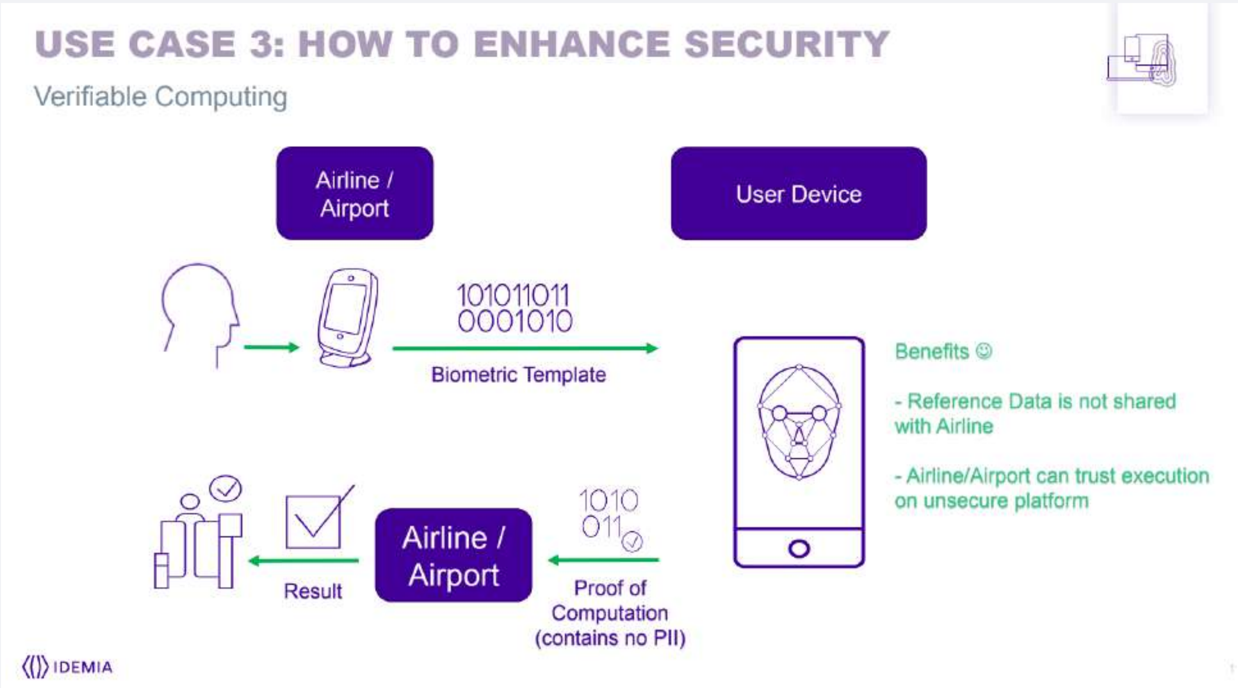
   In these types of architectures, the level of privacy can be enhanced through the use of **Full Homomorphic Encryption (FHE)** combined with **Secure Multipartite Computation (SMC),** which enable hosting personally identifiable information (PII) on a central storage without risk of leak or misuse. This ensures that the biometric identity provider cannot access the biometric data of the user, while still being able to use it for providing the specific service (i.e., securely monitoring access to a given territory).
2. **Personal devices.** For example, automated boarding at airports, tasking people with performing all necessary checks via their personal devices, e.g., smartphone. In this scenario, user reference data does not leave their device, offering a more privacy-friendly alternative for the person. However, the service provider (i.e., airline/airport) must trust execution on an unsecured platform (i.e. smartphone), and that the information provided by the user is correct.

In a world where technological development is accelerating, describing the essential requirements in functional and technical terms is better than mandating how technologies must be developed and deployed, as nobody knows what technologies and capabilities may appear in the future.

In such circumstances, a viable option is to integrate **Verifiable Computing** techniques within the system, providing the possibility to trust a calculation which has been performed by an unsecure/untrusted platform. In this scenario, computational processing is shared by all users, minimising the possibility of deceptive acts, thereby giving the service provider a high level of trust in the performed operation, despite it being executed on an unsecure platform.

Key takeaways. Mr Bouatou finished his presentation with the following messages, including:

1. protecting personally identifiable information (PII), and ensuring privacy requires an **approach tailored to each specific use case;**
2. the techniques and technologies currently in development, when combined and properly applied, will be able to solve many issues that are now considered to be **high-risk processing operations;**
3. in the context of continuous technological development, it is recommended to **describe the requirements of systems in terms of their essential functionalities,** instead of mandating how technologies must be developed or deployed, as this can stifle and limit innovation.



Session III

16 June 2022, Strasbourg (France) & online

Identity Management as a Service – Industry presentations

Chair:
Aleksandrs Cepilovs – Capability Building Officer, eu-LISA

Mobile Identity Verification. Technological Solutions for Self-service Systems in the Context of the Entry/Exit System

READID POWERED BY INNOVALOR

Robin Smits, Global Sales Director for ReadID at InnoValor

The presentation focused on solutions for remote verification of identity documents aimed at relieving part of the pressure at the EU's external border crossing points (BCPs) that are expected to occur with the launch of the Entry/Exit System (EES), and the European Travel Information and Authorisation System (ETIAS). In this context, a critical part of the solution to potential queues is empowering users to perform part of the process that would usually take place at the border, and do it from their homes using their smartphones to verify government-issued identity documents.

To set the scene, Mr Smits provided an overview of challenges associated with the introduction of EES and ETIAS, most of which, if not all, can be tackled by remote verification of identity documents:

- **increasing passenger traffic** after the lifting of pandemic restrictions,
- modernising the EU's border-crossing processes with the **introduction of EES and ETIAS,**
- improving to the **quality and efficiency of procedures** at BCPs,
- ensuring **balance between security and supervision** of travellers in the process.

NFC-based identity verification. The current practice of **manual evaluation of identity documents** is challenging due to the time constraints at BCPs, as well as the constantly evolving technologies used by criminals to produce counterfeit documents. The most reliable solution to this problem is the use of the **Near-Field Communication (NFC) technology,** which is at the core of InnoValor's ReadID solution offering a secure, scalable self-service for remote document verification.

How do passport chips work?

1. The smartphone scanner reads the **Machine-Readable Zone (MRZ)** of the ID document (e.g. passport), which contains alphanumeric information (i.e. document number, date of birth, date of expiry, etc.) that is used as a 'password' to access the **RFID (radio frequency identification) chip**.
2. The **RFID chip** is then used to **verify document authenticity,** by way of retrieving digitally signed personal information, i.e. name, date of birth, etc.

The ReadID application. Also **performs cloning detection** to make sure that the information on the NFC chip has not been copied. Smartphone is used only as a scanner, and all verification procedures are done externally to the device used by the end-user. The ReadID application performs verification of the identity document in two simple steps:

- **scans the MRZ and the Visual Inspection Zone (VIZ)** with the smartphone camera,
- reads the **RFID chip with the smartphone NFC reader** (or use the optical solution if no chip is available).

The extracted data is then sent to a trusted environment that will provide this verified data to Member State authorities, **ensuring that the data is correct and is retrieved from a verified document.**

ReadID provides trusted identity verification that leverages what people already have: government-issued identity documents with contactless NFC chips and NFC-enabled smartphones.

The data provided through this procedure includes:

- **biographical data,** i.e. name, gender, nationality, date of birth, personal number (optional),
- **biometric data,** i.e. high-resolution facial image, fingerprints (more challenging),
- **document information,** i.e. document number, document code, issuing state, date of expiry,
- **optional data,** i.e. full name (longer version, special characters), address, place of birth, iris, signature, etc.

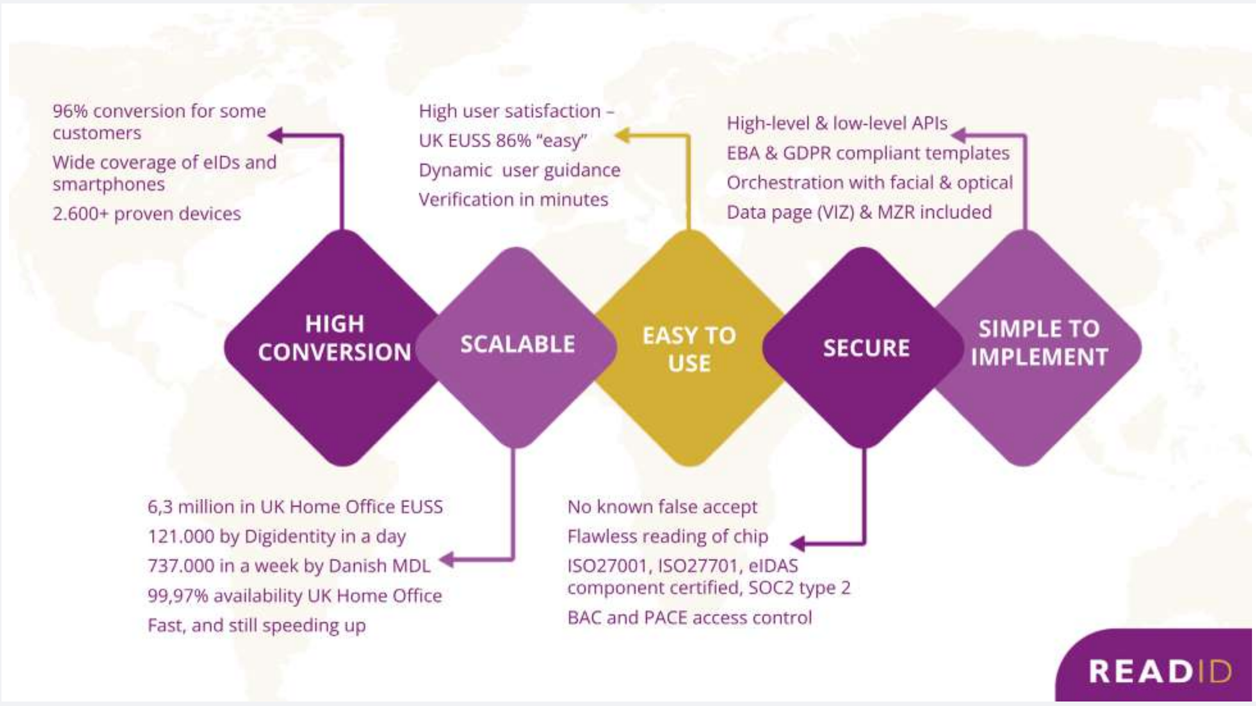
The use of RFID chip to retrieve data has several advantages, in particular when it comes to the verification of facial image, which in the context of optical evaluation is compared against an image of inferior quality. The use of the RFID chip also allows to retrieve additional information which is not available on the document's VIZ (depending on the country of issuance). Mr Smits then demonstrated the ReadID application in practice via the following video: youtube.com/watch?v=QP_6pWD5Qes

Advantages of the ReadID solution. In the context of remote identity document verification as part of the border-crossing procedure, the ReadID offers the following benefits:

- high customer conversion rate (96% for some customers),
- wide coverage of electronically-enabled identity documents (eIDs) and smartphones,
- the solution is scalable and fully automated,
- easy to use for the end users,
- highly secure,
- simple to implement.

In closing, Mr Smits outlined some of the more specific **mobile use-cases for EES/ETIAS:**

- **self-service / remote / pre-arrival:**
  - send in biometric data from the chip in ID document,
  - pre-check/classify third country nationals,
  - error-free and verified data,
  - optional: holder (face) verification.
- **empowering border officers / face-to-face:**
  - instant verification of identity documents,
  - data entry directly into the system, without typing or scanning errors,
  - use anywhere, i.e. suitable for remote environments, e.g. small land/sea BCPs.



iProov Genuine Presence Assurance

Andrew Bud, Founder and CEO, iProov

Mr Andrew Bud opened the presentation with a short introduction of London-based tech company iProov, a global leader in face-based authentication services with their Genuine Presence Assurance (GPA) solution, with up to one million daily verifications worldwide. GPA, developed by iProov is an eIDAS level High certified solution for unsupervised biometric enrolment that has undergone numerous government-level audits, incl. in the UK, the USA, Australia and Singapore.

Systematic security monitoring is absolutely fundamental for detecting biometric vulnerabilities. Verifying liveness and genuine presence are forms of cyber security defence but it is important to keep in mind that exploits are inevitable and threats keep evolving.

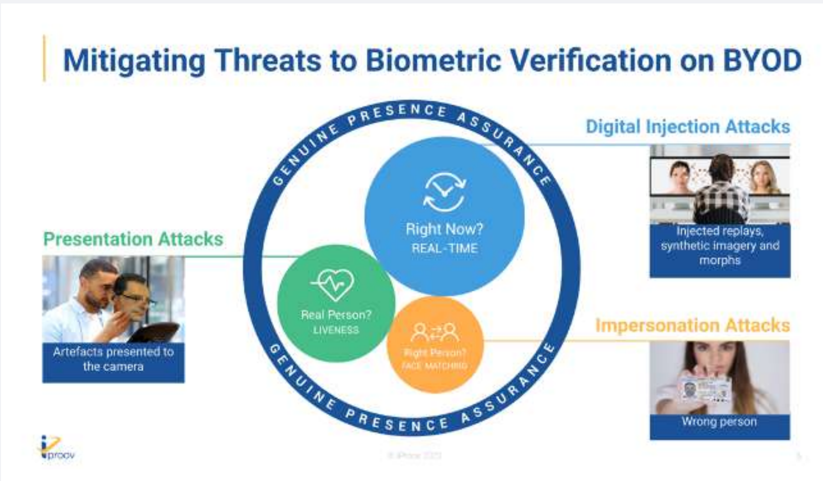
Multiple bottlenecks at BCPs. Mr Bud continued his presentation by outlining the key bottlenecks, such as limited space at many ports of entry as well as time necessary to process TCNs crossing borders, which will be **further exacerbated with the launch of the Entry/Exit System (EES),** introducing new data capture requirements. To alleviate some of the pain points, Mr Bud suggested to remove some of the **time-consuming and space-demanding processes** away from the BCPs – a supervised environment – to people's homes, which fundamentally is an unsupervised environment with untrusted hardware.

Securing trust from the couch. By moving a key process – identity verification – from the border gate to people's homes, the key challenge is to **ensure secure and private flow of biometrics and data from the couch to port** of entry/exit. Addressing this challenge requires solving two challenges:

- trusted capture of **ID document** with user's own device, e.g. InnoValor's ReadID solution,
- trusted capture of **facial biometrics** with user's own device, requiring two safeguards:
  * **genuine face assurance** – right person, real person, right now,
  * **protection against morphed selfies.**

Remote enrolment risks – attacks. In the case of remote enrolment, it is important to consider the possible multiple attack surfaces (incl. morphed selfie attacks), it is essential to ensure that only the identity of the genuine travel document holder is enrolled. To ensure that a genuine person is enrolled, three types of attacks need to be mitigated:

- **impersonation attacks**, i.e. wrong person,
- **presentation attacks** using physical artefacts during enrolment, e.g. masking,
- **digital injection attacks,** using synthetic imagery or morphs.



Protection against digital injection attacks. While existing technologies address only the first two types of attacks, iProov offers a solution that mitigates also digital injection attacks. iProov addresses all three types of attacks by injecting additional random information into the stream by using **controlled illumination** which cannot be replicated by the attacker. This information – the reflection of different colour light – is then streamed as video together with the facial image to the iProov server in order to ensure presence assurance.

Advantages. One of the advantages of the solution provided by iProov, is the effortless user experience, which allows for success rates in the heights of 98% in unsupervised biometric enrolment environments. The application is also being constantly **monitored for racial bias,** performing with statistical parity across different racial groups. In addition, iProov performs continuous security monitoring in order to identify any possible suspicious activity to ensure that the system **responds to the constantly evolving threats.**

Q&A session

Following the presentation, the audience raised a number of pertinent questions.

1. **Controlled illumination.** In response to the question on whether the set of **random light flashes** is fixed at 15 or can be variable, Mr Bud responded that currently the set is fixed at 15, which results in a number of options large enough to make it impossible to create galleries and inject those during an attack. The number can also be variable, but it should not be small, as this would allow the injection of pre-produced image galleries attempting to match colour patterns.
2. The follow-up question addressed the **support infrastructure.** Responding to this question, Mr Bud explained that security is ensured by performing all operations on iProov's **cloud-based infrastructure,** ensuring that none of the operations are performed on the untrusted devices of end-users. Requirements for data sovereignty, privacy and security means that iProov processes data in many parts of the world, operating over 30 different cloud instances worldwide. iProov software can be implemented on any cloud providing that it accepts **Kubernetes containers.** The solution can be implemented on premises, but this would require providing full access and control over the software to iProov in order to ensure constant security monitoring and regular updates in order to address any new exploits. The fact that the solution is cloud-based allows to make it highly scalable, assuming that the cloud service provider can handle the load.
3. The final question focused on **security monitoring practices** deployed by iProov. Considering that the iProov Genuine Presence Assurance solution is used across a wide range of services, including cryptocurrency wallets, it is highly likely that an exploit will first be identified in other applications and will be addressed before it reaches border control systems.

At-home Passenger Pre-enrolment and Smarter Border Control

Alejandro Aleman, ABIS Solution Manager, innovatrics

Mr Alejandro Aleman opened the presentation with a short introduction of Innovatrics, based in Slovakia. Since 2004, Innovatrics has been building hardware-agnostic Automated Biometric Identification Systems (ABIS), and developing expertise in different biometric modalities (i.e. face, fingerprint, iris), including face liveness detection. Their biometric algorithms have been consistently ranked among the best in the world in the assessments performed by the USA National Institute of Standards and Technology (NIST).

Digital onboarding. In order to alleviate the potential challenges at border crossing points that may arise with the launch of EES, Innovatrics has developed a remote onboarding solution for the **visa application procedure.** To set the scene, Mr Aleman elaborated on the key factors and technologies which are essential for the implementation of remote identity verification and enrolment:

- wide availability of smartphones,
- significant improvement in facial recognition technologies,
- significant improvement in liveness detection technologies, and
- desire to improve customer or traveller experience.

The **remote visa application** solution, developed by Innovatrics, removes the need for an applicant to travel to the capital or even to another country in order to apply for a visa, instead allowing to remotely enrol the necessary identity document information and facial biometrics.

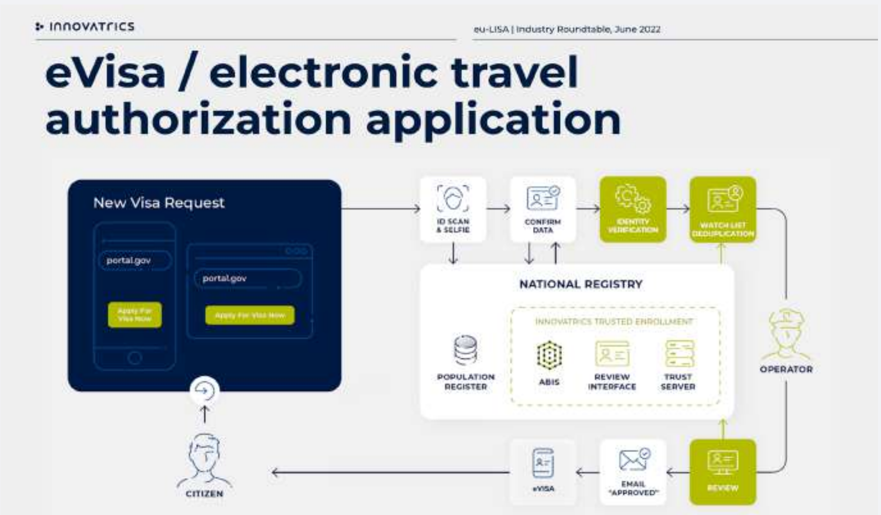
Document processing, comprising:

- **data extraction,** using the MRZ reader, Visual Inspection Zone reader (using OCR), barcode reader, and NFC capability to extract data from the RFID enabled identity documents;
- **document authenticity verification,** i.e. MRZ data validation against the data in the Visual Inspection Zone and/or RFID chip; field and picture authenticity; colour profile accuracy; validation of expiry date and photo, incl. age/gender using biometrics.

Liveness detection, using deep neural networks to detect a wide range of presentation attacks by focusing on three components: active, passive, smile. These can be implemented as stand-alone features or in combination, including both online and offline in applications where internet connection is not available or unstable.

Electronic visa/travel authorisation application. To exemplify how the solutions developed by innovatrics work in practice, Mr Aleman presented a use case of an electronic visa/travel authorisation application. The workflow involves the following steps:

1. **passenger self-enrolment,** i.e. taking a selfie and scanning an ID document,
2. if the passport is RFID enabled, the chip is read to retrieve the data and verify against the MRZ/VIZ data **in the national registry,** together with a cloning check,
3. the next step is **identity verification,** in conjunction with **watchlist deduplication,** both performed within the **innovatrics trust platform/server,**
4. finally, on the basis of the provided information and the results of verification, **system and process operators** will then **review and decide** whether to issue a visa or not.



With new technologies it is possible to provide a seamless and effortless service to the traveller, while also maintaining a high level of security.

Mr Aleman concluded his presentation by highlighting how remote biometric self-identification can provide a seamless service to the traveller, while also maintaining a high level of security.

In terms of **seamless service:**

- no need to visit embassy/visa office, i.e. time-saving effect + minimises potential health risks,
- improved customer experience,
- cutting processing time and reducing personnel costs.

As for **security benefits,** Mr Aleman highlighted the following aspects:

- advance knowledge about who is planning to enter the country before they appear at the border in person,
- background checks against blocklists,
- checks against previous travel records.

Verifiable Digital Travel Credentials and Seamless Travel

SITA

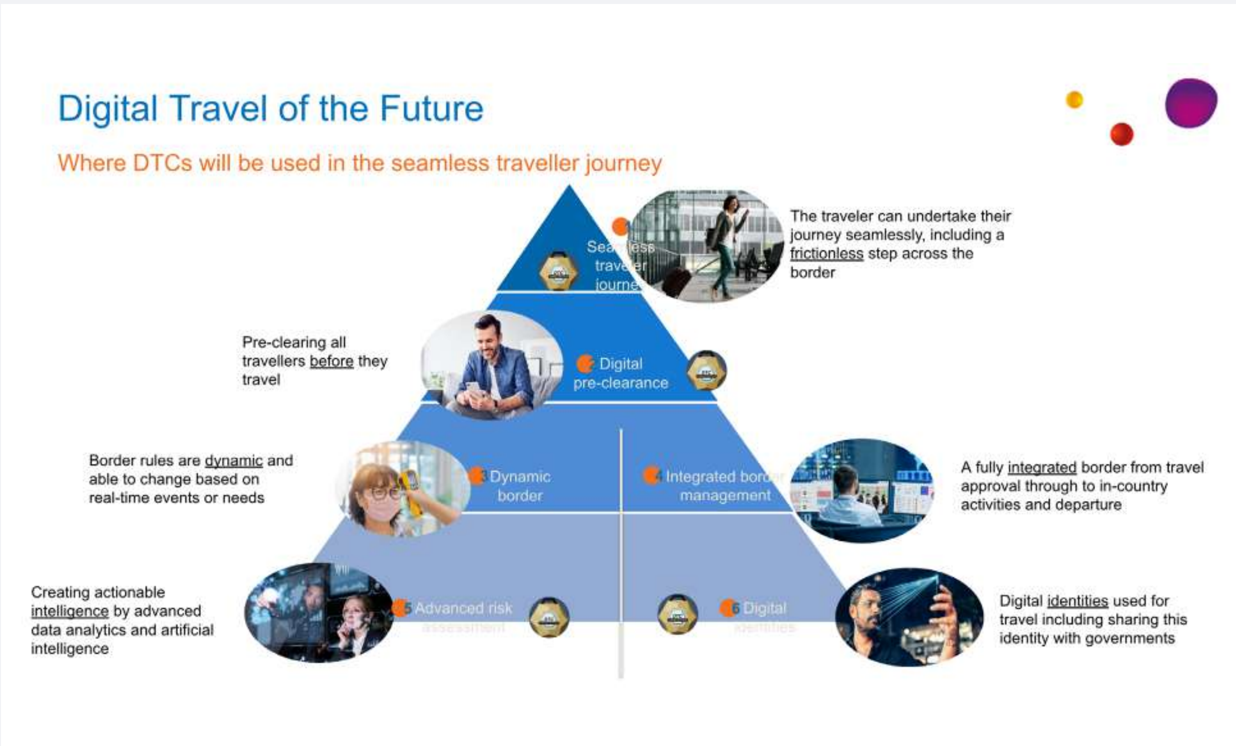
Andy Smith, Director, Government and Industry Relations, SITA

As the representative of SITA, the world's leading specialist in air transport communications and information technology, Mr Smith's presentation focused on the use of technologies to facilitate secure border-crossings from the point of view of air carriers.

The key to enabling seamless traveller experience starts with **advance provision of information** to the relevant authorities to ensure **pre-clearance of travellers** even before they reach the border. This, in turn, requires **trust** between the stakeholders involved in the passenger journey, and also towards the technologies that facilitate these processes.

To set the scene, Mr Smith provided an overview of scenarios where **digital travel credentials (DTC)** and **advance passenger processing** can help alleviate some of the bottlenecks. This is particularly pertinent in the case of additional checks, such as those introduced during the COVID pandemic, that have the tendency to create severe disruptions in passenger flows, especially if not backed by technology.

- **Redefining passenger pre-clearance from the perspective of border security.** Most commonly, pre-clearance focuses on designing and ensuring seamless traveller journeys. However, this process is equally important from the perspective border security, i.e. ensuring the timely identification of persons who shouldn't be allowed to cross the border. For example, in Thailand, SITA's pre-clearance systems have helped apprehend more than 155 persons in the first half of 2018;
- **Dynamic approach to border rules and procedures.** Prior to the COVID-19 pandemic, border rules were relatively static. In the aftermath, they have become much more dynamic and it would be preferable if it remained that way because modern technologies, such as DTCs, enable flexible response to world events, e.g. during pandemics;
- **Integrated border management.** Ideally a fully integrated process starting with pre-approval at home and ending with departure. In addition, travel data can be integrated with freight data, both rich sources of data to support intelligence. Integration should also be done across different modes of transport as well. When talking about actionable intelligence based on inputs produced by artificial intelligence (AI) and machine



learning (ML), we should never remove human beings as the final decision maker. In such cases, AI and ML should be relegated to what they do best, i.e. analysing large-scale datasets to provide relevant inputs to the decision maker for risk evaluation. The benefits include shorter wait-times at the border, allowing border control officers to focus on high-risk travellers;

- **Digital identities/DTCs.** Enabling information-sharing with government authorities, while also relieving carries from the responsibility of document and identity verification.

Such interactive capabilities and pre-clearance procedures are already used by a number of governments working with SITA. In addition, more than 500 airlines have been configured to support these procedures, that are transferable to other modes of transportation as well, e.g. cruise lines. The integration of biometric data in the pre-travel clearance procedure will **enable even further capabilities** for enhancing security and creating a more seamless traveller experience.

Digital identities and digital travel credentials will be a game-changer for our industry, and for the relationship between the travellers and governments as well.

Some examples from Australia. Pre-clearance has been effectively used to ensure safety and security for many years, e.g.:

- 25 years ago, Australia introduced **interactive Advanced Passenger Information** linked to the world's first electronic travel authorisation system, which together enabled a denial of boarding capability. This significantly reduced public costs of managing travellers not eligible to cross the border. Similar solutions were later used in South Africa during the football World Cup, helping protect the event from football hooligans:
- **Australian Electronic Travel Authority (ETA) app,** launched during the pandemic, is an example of integrating biometric data with electronic travel authorisation. The app comprises secure biometric authentication, passport chip reading using NFC technology, OCR scanner ensuring data integrity, and capture of live facial biometrics through a smart selfie functionality, allowing the creation of galleries for simplified arrivals.

In conclusion, Mr Smith stressed that all the technologies necessary to make this operational are already available. We should not be afraid of using technology that has already been proven to be effective, especially if taking such an approach will not only provide a more pleasant traveller experience, but will also help make our borders more secure. To that end, it is important to continue working closely with the industry, and to learn from experiences of other countries.

Q&A session.

Following the presentation, Mr Smith addressed the following questions:

1. **Liveness detection.** SITA's partner for liveness detection is biometrics company Aware. What is important, Mr Smith asserted, is to see the pre-enrolment process not as a final point. There are plenty of possibilities for relevant authorities to intervene even after pre-enrolment, thus ensuring that decisions are not made automatically and the process is secure.
2. **Regulatory framework.** Responding to the question of how to convince regulators of the safety of available technologies, Mr Smith assured that regulators have gradually changed their attitudes. He further stressed that regulators should not seek to be at the bleeding edge of technology, as this may create unnecessary risks, but at the same time, they should not be afraid of using technology that has already been proven to be effective. To that end, it is important to continue working closely with the industry, and to learn from experiences of other countries.

Processes to Accelerate EES Border Crossing Transaction Times

Matthew Finn, CEO, Augmentiq

Opening his presentation, Mr Matthew Finn from security innovation consultancy Augmentiq, emphasised the importance of **collaboration between different stakeholders** operating in the travel and border crossing context, e.g. government authorities, carriers and technology providers. It is also extremely important to **share information about technological capabilities** to learn from successful case studies developed around the world. This is important, as **we normally tend to think about these processes in isolation,** which often results in processes that are misaligned, resulting in a significant impact on carriers. In this context, it is important to always bear in mind that **someone's outbound traveller is an inbound traveller somewhere else.**

Eurostar EES impact case study. The presentation focused on the potential impact of EES on border-crossing processes and carrier operations, based on the modelling exercises performed in 2019, together with Eurostar and a EU Member State. At the MS level, the tests focused primarily on the efficient operation of back-end systems, while also highlighting aspects that are likely to be overlooked, e.g. stakeholder collaboration, operating procedures, new tools, staffing schedules, and future proofing.

As for Eurostar, there is no scenario in which EES does not have a **significant negative impact** on Eurostar's operations. Additionally, simulations by the French Ministry of the Interior modelled high-volume scenarios in which as many as 80% of travellers could be subject to EES. In such cases, on peak days of operation, EES processes could add more than 5 hours of queues at the St Pancras International station in London, and 3-4 hours at the Gare du Nord in Paris. More specific estimates show that for first-entry passengers, EES requirements will increase processing time by 285%, which is not sustainable. Hence, it is essential to **minimise the processes that take place at the station** on the day of travel by upstreaming maximum data capture prior to the day of travel via **leveraging self-service systems,** i.e. online, mobile, kiosk, to **reduce congestion and overcrowding at BCPs.**

When considering how to improve these processes, one of the main stumbling blocks was a condition inscribed in the **EES legal base** that stipulates **only one option for the pre-enrolment of passenger data** – using on-site kiosks under the supervision of border guards. However, nowadays, kiosks are not the only option for the pre-enrolment of data prior to border crossing. Other options include **various online or mobile solutions** that can facilitate different aspects of the border check processes, incl. document authentication, facial image capture, filling out the Schengen questionnaire, passenger data capture (e.g. API, EES) and any supplementary data capture (e.g. health certificates, ETIAS record numbers, etc.). Nearly all of these can be captured and securely verified via self-service systems prior to the day of travel and away from the BCP. Nevertheless, there will still be a need for additional checks and enrolment of fingerprints on the day of travel at the BCP. However, self-enrolment will significantly reduce the scope of actions to be undertaken at BCPs, thereby also minimising passenger processing time at the border.

Main takeaway. Regulations should be **outcome-focused and capability-driven, specifying what needs to be done,** rather than detailing how things should be done. Excessively prescriptive regulations have a tendency to **lock development into a specific pathway,** which may hinder us from taking an alternative approach, e.g. applying new technologies that could better achieve the stated objectives.

It is essential to minimise the processes that take place at the station on the day of travel by upstreaming maximum data capture prior to travel.

Q&A session

1. **Regulatory framework.** The first question challenged some of the conclusions put forward in the presentation, specifically on readiness to adopt new technologies for pre-enrolment. According to Mr Finn, these conclusions are based on recently-performed evaluations, which involved discussions with regulators, leading to the assessment that kiosks are still the only feasible option within the current legal framework. However, he expressed hope that governments will

be increasingly more open towards incorporating new technologies and re-designing processes to allow for pre-registration in order to address some of the challenges that we are bound to facing, e.g. a three-fold increase in processing times for first-time EES passengers crossing Schengen borders.

2. **Processing time.** A follow-up question focused on the distinction between analysing processing times at devices against analysing processes in real-life environments, where processing is further prolonged by a lot of friction points. In response to this question Mr Finn, explained processes need to be analysed in operational environments in order to estimate real processing times. In this context, **time and motion studies** are absolutely essential for evaluating actual impact. One of the issues faced in discussions around transaction times is that people often consider transaction times that are 2 seconds long as negligible. However, if we sum up a couple of such negligibly short transaction times, we already have 10 seconds. Then, if we multiply it by 900 passengers (Eurostar maximum capacity), we will come to the conclusion that we will need an additional 2.5 hours for boarding the train, while the current time-window for border crossing is 45 minutes.

Closing Remarks

Krum Garkov, Executive Director, eu-LISA

In his closing remarks Mr Garkov emphasised that technologies, including biometric identity management and biometric recognition technologies, are developing at a very fast pace, which leads to a significant **gap between technological capabilities and the regulatory framework.** This gap needs to be addressed as a matter of priority, otherwise we will fail to utilise the technological capabilities that are already available.

Mr Garkov also stressed that technologies are, in a sense, neutral – they don't solve problems by themselves, but are only tools that can help us solve the challenges we face. When talking about new technologies, we always need to think about re-designing processes, **re-thinking the ways we operate,** which requires additional capacity building.

With the evolution of EU's border management and internal security systems, the EU and Member States need **end-to-end integrated solutions,** not disparate bits and pieces. At this event, we've seen a number of components of integrated solutions, what we need to do now is to integrate these components not only in the technology layer, but also into operational processes. This is the only way we can ensure that technologies actually improve the efficiency and effectiveness of operational activities on the ground.

Another takeaway mentioned by Mr Garkov was that border management and internal security challenges, as well as their solutions, are very similar across the globe. This suggests that we **don't have to reinvent the wheel,** instead we must **focus on reinforcing international collaboration.**

The gap between available technological capabilities and the regulatory framework needs to be addressed as a matter of priority.

Finally, Mr Garkov emphasised that trust is one of the key challenges in identity management and biometrics. No matter how good the technologies are, if citizens don't trust that technologies are used responsibly and for legitimate purposes, we are bound to face setbacks. Therefore, we need to **balance our excitement about new technologies with proportionate safeguards** that must be put in place in order to ensure data protection and privacy, in order to gain public acceptance for the use of these technologies. Only then will we be able to reap the benefits these technologies have to offer.

ISBN 978-92-95227-05-7
ISSN: 2600-2728
doi:10.2857/647326