

IDENTITY MANAGEMENT TECHNOLOGIES

IN THE CONTEXT OF INTERNATIONAL TRAVEL AND MIGRATION

eu-LISA Research and Technology Monitoring Report September 2025

Contents

Executive summary	4
1. Introduction	7
1.1 What is identity?	7
1.2. How is a legal identity established?	10
1.3. What is identity management and verification and where is it used?	11
1.4. How has identity management changed through time?	12
1.5. A brief history of travel documents	14
2. Identity management in the EU and the role of eu-LISA	19
2.1. Digital identity and digital identity wallets	19
2.2. eu-LISA large-scale IT systems and identity management	22
2.3. Interoperability architecture and components	24
3. Identity management technologies for cross-border travel	31
3.1. Remote enrolment of identity information	31
3.1.1. Digital Travel Credentials	32
3.1.2. The EU Digital Travel Application – proposal for a Regulation	34
3.1.3. Remote enrolment of identity data beyond the DTC: opportunities and challenges	42
3.1.4. The risk of presentation attacks in the remote enrolment of biometrics	44
3.2. Solutions for fraud detection in identity documents	47
3.3.1. Blockchain for identity management and verification	51
3.3.2. Some examples of digital identity wallet implementations	53
4. Technologies enabling access to humanitarian services for undocumented individuals	57
4.1. The use of blockchain in asylum context	59
4.1.1. Blockchain for assistance in asylum procedure – Germany	59
4.1.2. Blockchain for access to banking and financial inclusion	60
4.1.3. Blockchain for the streamlining of humanitarian aid towards ID recognition	61
Conclusion	62

Executive summary

Identity and identity management in a digital era

This Research and Technology Monitoring Report provides an overview of the evolution of identity management technologies in the context of international travel, migration, and border management. As global mobility increases and the digitalisation of public services accelerates, identity systems that are secure, interoperable, and respectful of rights have become foundational to effective governance, security, and access to services.

Over the past decade, the European Union has entrusted to eu-LISA the development and operational management of a complex architecture of large-scale IT systems that support identity management for security, migration, and cross-border mobility.

These systems capture, store, and process biometric and biographical data for third-country nationals interacting with EU borders and migration systems. The report outlines how eu-LISA's evolving portfolio ensures both data integrity and service continuity, even as new regulatory frameworks and technologies reshape identity management practices.

To overcome the limitations of systems working in silos, the EU has introduced a robust interoperability architecture to enable cross-system verification of identities and facilitate seamless access for law enforcement, asylum, and border authorities while respecting data protection and the relevant regulations. The implementation of the interoperability framework marks a paradigm shift, enabling near real-time identity checks across systems and improving the detection of fraudulent or duplicate identities.

Emerging technologies and innovations in identity management

The report presents a number of new technologies and innovations that support and facilitate modern identity management:

Digital Travel Credentials (DTC): Developed under ICAO standards, DTCs enable travelers to store a digital version of their passport on a secure mobile device, which can be pre-verified before border crossings.

Remote enrolment solutions: Leveraging personal devices (e.g., smartphones) for biometric and document data capture allows identity information to be submitted prior to travel, reducing congestion at border crossing points and increasing traveler convenience.

Digital identity wallets and Self-Sovereign Identity (SSI): New models of digital identity allow individuals to control their credentials and data-sharing preferences while enabling access to public and private services across borders.

Blockchain applications: Deployed for example in humanitarian contexts to support identity verification for undocumented or displaced individuals, enhancing access to services while preserving privacy.

Recent regulatory developments

The report presents the latest regulatory developments that support identity management:

IDAS and eIDAS 2.0 Regulations: Establishing a framework for cross-border digital identity and introducing the European Digital Identity Wallet, which will support secure digital identity for EU citizens and residents.

Proposal for a Regulation on the EU Digital Travel Application: Adopted in October 2024, this introduces an electronic travel application allowing advance submission and verification of identity data.

Digitalisation of Visa Procedures Regulation: Will enter into force in 2028, allowing for a fully digital visa process and potential integration with digital wallets and DTCs.

These legal instruments support the secure digital transformation of identity verification across border management, visa, and migration domains.

Risks and resilience in identity verification

The proliferation of remote enrolment and biometric identification technologies brings new risks related to fraud, security, and reliability, including: Presentation attacks (e.g., masks, printed photos); Morphing attacks (altered biometric data); Digital injection attacks (AI-generated or manipulated inputs).

To mitigate these threats, new techniques such as Presentation Attack Detection (PAD) techniques, biometric liveness detection, and AI-enhanced fraud detection tools are being deployed. EU-funded projects such as D4FLY and iMARS also contribute to innovation, by providing advanced tools for assessing document authenticity and detecting manipulation in identity images.

The road ahead: strategic considerations

To guarantee that new developments in identity management are fully successful, key priorities include:

- Ensuring data privacy and fundamental rights are upheld in every identity management process.
- Investing in robust fraud detection and biometric validation technologies.
- Coordinating Member States and stakeholders on common standards and interoperability.
- Continuing to assess ethical and societal impacts, particularly for vulnerable populations such as asylum seekers or the undocumented.

1

INTRODUCTION

1. Introduction

eu-LISA is a major player in identity management at EU level, in particular in the areas of visa, asylum, migration, and internal security, currently operating three large-scale IT systems: the Schengen Information System (SIS), the European Asylum Dactyloscopy Database (Eurodac), and the Visa Information System (VIS)¹. Each of these systems includes identity management functions for a specific business domain. In addition to the above mentioned systems, eu-LISA is also responsible for the operation of the European Criminal Records Information System's Reference Implementation (ECRIS-RI) and e-CODEX. The implementation of the new systems, namely the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), and the interoperability architecture will be gradual in line with the decisions made by the Justice and Home Affairs Council. Similar to the systems already in operation, the new systems will also contain identity-related information and will therefore be part of the identity data landscape under the Agency's responsibility. With the entry into operation of the new Eurodac system based on the recast Eurodac Regulation², and the accompanying regulations which are part of the Pact on Migration and Asylum, Eurodac will increase its scope in the identity management ecosystem managed by eu-LISA. eu-LISA will therefore continue to be an increasingly important actor in the area of identity management in Europe. The Agency will also continue to rely on a wide range of technologies that are used to facilitate identity management processes. These technologies are constantly evolving, providing new opportunities to facilitate identity management. This report aims to shed light on the evolution of identity management over time, the role of eu-LISA in managing identity data, and the technologies used in these processes. The report covers a variety of topics in the area of identity management, starting from the definition of identity and identity attributes, to the most recent advances in some of the technologies, such as biometric recognition and self-sovereign identity.

1.1 What is identity?

The right to a legal identity is a fundamental right recognised in the international law³ and is intrinsically connected to many derived rights, such as the right to name, nationality, family, culture, and other rights⁴. Identity can be defined as a mix of biometric and biographic characteristics that are linked to a particular person. Some of these features (e.g., biometrics) are unique, while other (e.g., name, date and place of birth) can be shared with other individuals. Identity is normally established in a linear way, where at the most basic level the key document is the birth certificate, which confirms that a particular

¹ At the time of publication of this report.

² Regulation (EU) 2024/1358, OJ L, 2024/1358, 22.5.2024

³ E.g. the Convention on the Rights of the Child and the Universal Declaration of Human Rights

⁴ <http://scm.oas.org/pdfs/2007/cp19277.pDF>

person was born on a particular date in a particular place, to particular parents, and was given a specific name. In that sense, existence of a functioning civil registration system is an essential precondition to establishing a person's legal identity.

“ ***Identity can be defined as a mix of biometric and biographic characteristics that are linked to a particular person*** ”

When issuing identity documents such as identity cards, passports or driver's licenses, the data contained in the birth certificate or in the civil register is linked to biometric data, such as a facial image and, more recently, also fingerprints. At the other end of the line comes a point in time when a person is deceased and identity of the individual is closed.

Although on the surface this process may appear to be quite straightforward, in practice, establishing and verifying a person's identity with

high certainty has proven to be a complex process, as a person's identity is a dynamic and ever-evolving network of information, which may be specific to the local context and the requirements embedded in the traditions and legal systems of particular States. Identity-related information can be split into two sets: core identity attributes and other identity-related information. To complicate this further, a wide range of data sources and methods can be used for identity verification (see Figure 1)⁵.

When looking at Figure 1, it becomes clear that throughout a person's lifetime identity-related information, including some of the core identity attributes, may change multiple times. For example, depending on the jurisdiction, it is often possible to change one's name given at birth to any other name.

A person's name can also change as a result of marriage and divorce. Spelling of the name can change due to the adoption of new transliteration schemes by national authorities, which may affect, for example, transliteration from Cyrillic to Latin characters. Similarly, as we age, our biometric characteristics also change, adding another layer of complexity to identity verification. As for other identity-related information, such as passport numbers, addresses, bank records, etc., tracking these details to assemble sufficiently robust evidence to establish one's identity is an extremely complex undertaking. Technologies that help to address those challenges will be discussed in this report as they pertain to the field of 'identity management'.

5 ICAO, 2018 - <https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidence%20of%20Identity.pdf>

IDENTITY-RELATED INFORMATION, SOURCES, METHODS FOR VALIDATION

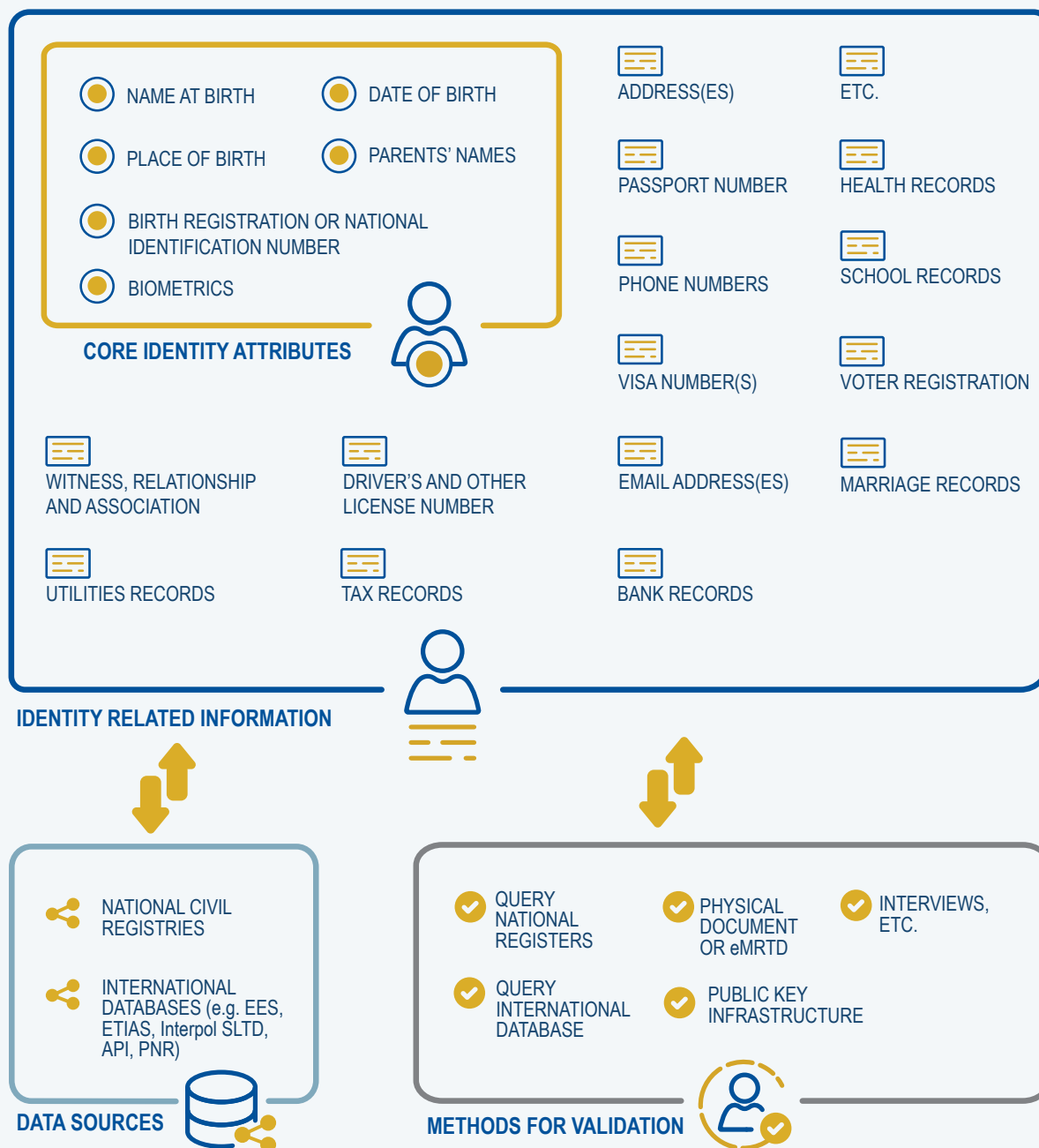


Figure 1: Identity-related information, sources and methods for validation (adapted from ICAO, 2018)

1.2. How is a legal identity established?

The first step towards establishing a person's legal identity is the birth of the person. Shortly after birth, the fact is registered in the civil register and the first document certifying the identity of the person – a birth certificate – is issued. In some countries, such as Estonia, a paper-based birth certificate is not issued; instead, upon registration in the population register⁶, the person receives a personal identity number, which is then used by public authorities when providing services to the individual. When creating a record in the population register, the identity of the newborn is linked to their parents or their legal guardian, and other identity-related information is recorded, such as the date and place of birth and the given and family names. The birth certificate, which represents a record in the population register of the country of birth, can then be used when acquiring any other identity document that will be issued subsequently. Today, when national identity documents,



Today, when national identity documents are issued, biographical information is linked with biometric information

such as passports or identity cards are issued, biographical information contained in the population register is linked with one or another kind of biometric information. Historically, before the creation of photography, the primary biometric characteristic used in identity documents was the bearer's signature. Later, portrait photographs were added to identity documents, followed by fingerprints with the creation of electronic machine-readable

travel documents (eMRTD). Depending on the age of the person, biometric information may be limited only to face (for children under a certain age) or contain both facial images and fingerprints (or other biometric information if provided for by the law). This way, biographical information which may be shared with other individuals, is bound to biometric information, which is unique for a particular individual (especially when a combination of several biometric trait is used). Binding biographical and biometric information allows for the verification of an individual's identity with a higher level of certainty.

While in some predominantly high-income countries, population registers are well-functioning and comprehensive, throughout numerous countries worldwide, civil registers either do not exist or do not cover significant parts of the population. According to the UN's Sustainable Development Goals Report from 2019⁷, less than half of all children under five years of age in sub-Saharan Africa are registered. As a result, according to recent estimates by the World Bank, approximately 850 million people cannot prove their legal identity due to the lack of recognised identity documents⁸. This limits opportunities for these people to participate in modern society, excluding them from financial services, public and social services, formal healthcare, formal labour market, as well as

⁶ Often also called civil register. Some countries also use the term civil registry.

⁷ <https://unstats.un.org/sdgs/report/2019/The-Sustainable-Development-Goals-Report-2019.pdf>

⁸ <https://id4d.worldbank.org/global-dataset>

opportunities to cross borders legally. Similarly, around 50% of deaths that occur around the world are not registered, thus not terminating existing legal identities. This opens opportunities for identity fraud, when identity information and identity documents of deceased individuals are misused with criminal intent.

Especially challenging is establishing a legal identity of migrants who cross borders without travel documents or any other identity documents (e.g., asylum seekers). In the absence of documentary evidence, authorities use a wide range of methods to establish an individual's identity. These methods include:

- Cooperation with third countries, including missions abroad and consultations with country liaison officers based in the (presumed) country of origin (often not feasible, especially in cases of refugees, or in countries without a properly functioning population register and identity management system).
- Comparison of biometric data (face and fingerprint) with data stored in relevant European databases.
- Analysis of data stored on smartphones and other electronic devices, as well as analysis of social media presence.
- Analysis of identity-related electronic and paper-based transactions with public authorities and private companies (such as banks).
- Interviews and language analysis to determine probable country and/or region of origin;
- Age assessment.⁹

Combining the results of analyses conducted using the methods indicated above may provide some level of certainty regarding an individual's claimed identity, based on which a new identity record can be created, binding claimed biographical information with biometric characteristics.

1.3. What is identity management and verification and where is it used?

Identity management, in its most primitive sense, is at the core of a functioning modern State as it provides a basis for population and tax registers and is essential for the delivery of most public services, such as education, healthcare and issuance of identity and travel documents. Identity management is also a basic precondition for a functioning democracy, as it is essential for voter registration and voter lists. During the past 20 years, as more and more government services have been digitised, digital identity

⁹ https://home-affairs.ec.europa.eu/system/files/2020-09/00_eu_synthesis_report_identity_study_final_en_v2.pdf (pp.30-31)

management has become central to public service delivery. It is also important for the delivery of private services where validation of the customer's identity is necessary (e.g., financial services, healthcare). Therefore, one can say that identity management is at the core not only of the modern state, but also an essential part of our day-to-day lives.

So, what is identity management and why is it so important? Identity management refers to the processes involved in the issuance of proof of legal identity to individuals by a government-authorized entity, as well as the maintenance of systems for managing the information and documents associated with such identity¹⁰. Such decisions range from eligibility to receive child benefits to border crossing, to entitlement to free parking and everything in between. Often, in order for an organisation to make a decision on whether to grant a right or to provide a certain service or not, the organisation performs verification of a person's identity. Identity verification can be defined as a process during which the authenticity of claimed identity data is verified against any other available source of identity data (e.g., passport, ID card, civil registry, etc.).

“ ***Identity management provides a basis for population and tax registers and is essential for the delivery of most public services*** ”

Identity verification processes vary depending on the use-case. In some contexts, such as the creation of a social media account, identity verification is often considered unnecessary or optional. In other environments, authentication of an individual's identity is highly regulated and tightly controlled. The latter category includes, for example, financial services, cross-border travel, as well as the provision of almost any public service in most countries. Risk assessment is therefore an essential component when defining requirements for identity management systems in different contexts.

1.4. How has identity management changed through time?

Throughout history, documents functioning in a manner resembling today's identity documents were issued to a small group of individuals, granting them certain privileges or status. Such documents could, for example, certify the status of a citizen in an ancient city-state or gave the bearer the right to safe passage through certain territories in medieval Europe. These documents could take various forms, including written documents signed by kings, as well as tokens or seals¹¹.

¹⁰ Access to Digital Identity for People on the Move in Europe (2023) International Organisation for Migration. <https://publications.iom.int/system/files/pdf/pub2023-075-r-access-to-digital-identity.pdf>

¹¹ Caplan, J. and Torpey, J. eds., 2002. Documenting individual identity: The development of state practices in the modern world. Princeton University Press.

Similar to the precursors to modern identity documents, population registers also have a long history, dating back to the register of households and individuals during the Han Dynasty in China in the second century BC¹². In Europe, population registers date back to the 16th-17th century, when the first population registers of individual parishes were recorded by the Lutheran church in today's Sweden¹³ and Finland. These contained records of married couples, newborn children, deaths as well as arrivals and departures from the parish. Local population registers gradually spread throughout Europe and beyond during the 19th and early 20th century¹⁴.

The need for a more comprehensive system of identity management to cover the majority of the population is connected to the rise of nation-states throughout the 19th century. Following the Industrial Revolution and with growing urbanisation, governments especially in Europe needed to create means for managing populations (e.g., to distinguish between residents and migrants) and to deliver nascent public services. The development of the early welfare state systems led to increasing bureaucratisation of government and the need for record keeping, which included the creation of identity documents, such as national identity cards. Similarly, many European nation states introduced military conscription, which required the creation of an effective system to manage military service, including the distribution of veteran's benefits. With the expansion of democratic participation through the 19th and the early 20th century, the need for effective identification of eligible voters further cemented the importance of identity management for the effective functioning of a modern society¹⁵.

Throughout this time, identity management through population registers, as any other record-keeping, was done using paper books. Centralised record-keeping in population registers was complemented by the issuance of identity documents, such as national identity cards and travel documents, which were used to verify a person's identity in the context of the provision of public services or when crossing national borders. Throughout the second half of the 20th century, some countries gradually introduced central population registers. The first country to do so in Europe was Iceland, which did so in 1953 at a time when registers were kept manually. This was possible due to Iceland's small population. With the introduction of electronic data processing (EDP), centralised population registers were implemented in many countries. One of the first countries to implement EDP in population register was Sweden in 1966. The implementation of the EDP was facilitated by the use of personal identifying numbers, which was introduced in Sweden in 1947. Other countries have introduced similar personal identifying numbers (PIDs) to facilitate identity management and provision of different services. Some countries

12 <https://www.osce.org/files/f/documents/7/d/39496.pdf>

13 https://unstats.un.org/unsd/demographic/meetings/wshops/1995_Rabat_CRVS/Docs/Doc.28_Sweden.pdf

14 Poulain, M., Herm, A. and Depledge, R., 2013. Central population registers as a source of demographic statistics in Europe. *Population*, 68(2), pp.183-212.

15 Caplan, J. and Torpey, J. eds., 2002. *Documenting individual identity: The development of state practices in the modern world*. Princeton University Press.

introduced a single personal identifying number which is used across all public and private services, whereas other countries, in particular those that do not have centralised population registers, use different personal identifying numbers for different services (e.g., separate PIDs for healthcare and tax management)¹⁶.

With the development of information technology and widespread adoption of the Internet, governments across the world have been gradually adopting information technology for the purpose of identity management. For example, Estonia mandated the use of electronic identity cards as early as 2002, which allowed it to develop a comprehensive ecosystem of digital government services, which since 2005 include the possibility to vote online. In 2014, the first edition of the eIDAS regulation¹⁷ (see section 2.1) entered into force, allowing, among other provisions, the recognition of electronic identification in the provision of digital services across borders. This, of course, is only possible thanks to the existence of comprehensive identity management systems at Member State level. The most recent development in identity management is the shift to decentralised identity management architectures, and in particular self-sovereign identity, which is also covered in this report.

In the context of cross-border travel and migration, for the most part authorities have been relying on travel documents for identity verification at border crossing points. This includes verification of individual's identity using a combination of biographical and biometric information (facial image, with the later addition of the possibility to check fingerprints included in the eMRTD), as well as verification of the eligibility to cross the border using visa stamps. With the widespread use of electronic databases, and in particular with the diffusion of the internet, countries started to increasingly deploy digital systems for identity verification, including the verification of records in visa databases to facilitate border checks and prevent visa fraud. The most recent development in this area is the creation of similar systems for visa exempt travellers (e.g., ETIAS in the EU, ESTA in the US, etc.), as well as the creation of entry and exit systems (e.g., EES for the Schengen area) to facilitate and control cross-border travel, which perform the function of an identity management system containing biographical and biometric information deployed for a particular purpose.

1.5. A brief history of travel documents

Travel documents remain essential for identity verification in cross-border travel. For much of the time that humans have existed, they have not had to prove their identity, or, at the very least, have not had to use documents to prove their identity. This can be largely explained by the fact that until the emergence of agriculture and larger settlements, people lived in small settlements where everyone knew everybody, which made

16 OSCE ODIHR, 2017. Compendium of good practices in identity management in the OSCE region

17 Regulation (EU) No 910/2014. OJ L 257, 28.8.2014, p. 73–114

identity verification unnecessary. The need for individual identification with a portable document largely arose as a result of the need to identify persons who travelled outside of the boundaries of the place where they lived. According to some sources, documents functionally resembling passports existed already around 450 BC and were used solely in the context of what today would be considered cross-border travel¹⁸. In the Western world, the origins of modern passports can be traced to mid-13th century¹⁹, when certificates of safe conduct were issued by either a local landlord, a military officer or an administration in order to allow for safe passage through foreign lands. Initially, certificates of identity, which were often represented by a letter of introduction or safe-conduct, were only accessible to diplomats, carriers and merchants. Regular travellers could only access such documents at great expense²⁰. The laissez-passer (Fr.) or passaport (It.) evolved into widely recognized travel documents with time. Already in the 16th century, the documents certifying one's origin and identity became essential to an increasingly large group of people. By the early 18th century, travellers not bearing an officially issued identity document could be subjected to significant penalties.

TYPE OF "INTERNATIONAL" OR "STANDARD" PASSPORT
RECOMMENDED BY THE LEAGUE OF NATIONS PASSPORT
CONFERENCE HELD IN PARIS IN OCTOBER 1920. (The model
is that of a passport such as would be delivered by the Spanish Government.)

<p>Este pasaporte contiene 32 páginas Ce passeport contient 32 pages</p> <p>Visas de l'Union des pays</p> <p>PASAPORTE PASSEPORT</p> <p>NOMBRE DEL PAIS NOM DU PAYS</p> <p>Nº del pasaporte Nº du passeport</p> <p>Nombre del portador Nom du porteur</p> <p>Asignación de su signo Affectation de son signe</p> <p>Accompañar de su familia Accompagner de sa famille</p> <p>NACIONALIDAD NATIONALITE</p>	<p>SEÑAS PERSONALES SIGNALEMENT</p> <p>Profesión Profession</p> <p>Longitud y fecha de nacimiento</p> <p>Sexo y edad de nacimiento</p> <p>Donación Donation</p> <p>Raza Race</p> <p>Color de los ojos Couleur des yeux</p> <p>Color de la piel Couleur de la peau</p> <p>Color de la cabeza Couleur des cheveux</p> <p>Signos particulares Signes particuliers</p> <p>HIJOS - ENFANTS</p> <p>Nombre Nom</p> <p>Edad Age</p> <p>Sexo Sexe</p>
<p>Esposa Femme</p> <p>(photo)</p> <p>(Foto)</p> <p>Imbre SEC</p> <p>FIRMA DEL PORTADOR SIGNATURE DU TITULAIRE</p> <p>Y DE SU ESPOSA ET DE SA FEMME</p> <p>Firma del Expediente Signature de l'agent délivrant le passeport</p>	<p>Puede en las cuales este pasaporte es válido Peut être dans lesquels ce passeport est valide</p> <p>La validez de este pasaporte termina Ce passeport expire le</p> <p>a menos que se renueve à moins de renouvellement</p> <p>expirado en admis a fecha date</p> <p>RENOVACIONES RENOUVELLEMENTS</p> <p>1º 2º 3º</p>

The exact size of this passport should be: 13 1/2 x 10 1/2 centimetres.
The passport is to contain 32 pages. The first four pages only are reproduced herewith.
The other 28 pages should all be numbered and should contain the visas of the countries for
which the passport is valid. The passport should be drawn up in at least two languages,
i.e., in the national language and in French. The passport must be bound in cardboard,
bearing on the top the name and in the centre the coat of arms of the country, and at
the bottom the word "Passport", with the addition, according to the desire of the various
Governments, of any practical information concerning the regime of passports. Any
passport of which the pages are entirely filled must be replaced by a fresh passport.

Figure 2: League of Nations passport

During the second half of the 19th century, with the rise of liberalism, many countries across the Western world abandoned the requirement to carry passports when crossing borders, although passports were still issued. During this period, passports and other identity documents were largely used to verify identity in the delivery of certain services (e.g., at post offices or when converting foreign currencies at local banks). Such a liberal regime of international travel existed until the First World War when stricter controls were introduced at national borders. Up until WWI, passport issuance around the world was also not standardised. Only after the WWI, which unleashed massive migration flows across Europe and beyond, a coordinated approach to controlling migration, verifying identity at the border, as well as identity documents, was

18 See Lloyd, 2003 (The Passport: The history of man's most travelled document)

19 See e.g., Clanchy, 1993

20 Groebner, 2001 in Documenting Individual Identity

deemed necessary in order to facilitate control during passengers' journeys. The agreement on a uniform style of passport was reached by the International Conference on Passports, Customs Formalities and Through Tickets called by the League of Nations in 1920. Such uniform passports (Figure 2)²¹ have been a permanent feature of international travel and the key document for identity verification for the past 100 years. The proposed standard passport included the following information:

- The first page included the name and coat of arms of the issuing country, an official government stamp, the number of the passport, name of the bearer, his spouse's name if accompanying, number of children and the bearer's nationality.
- The second page contained personal identifying information about the individual and his spouse, including profession, place and date of birth, country of residence, colour of eyes and hair and any other special characteristics. At the bottom of the page, additional information about the children could be included, including name, age and gender.
- Page three contained facial images and signatures of the passport holder and his spouse. The images were officially endorsed with a stamp. This page also contained a signature of the issuing officer.
- The fourth page included information about the countries where the passport was valid, the place and date of issuance, as well as the date of expiry²².

Little has changed since the introduction of a standard passport format in the 1920s in terms of information contained with the exception of the addition of fingerprints on biometrically-enabled electronic machine-readable travel documents (eMRTD). Early versions of passports contained the main biometric identifier used to this day, namely the facial image. What has changed, however, is the way information is presented and the security features of passports. The first significant evolution in travel documents was the introduction of a machine-readable zone (MRZ) in a travel document (Figure 3)²³, which allowed to use computers enabled with optical character recognition to read the passport, thus significantly reducing the document processing time²⁴.

The second major evolution in the development of travel documents was the integration of a radio-frequency identification (RFID) chip in a passport. This contained all compulsory and optional data presented in the visual inspection zone, biometric information (i.e., facial image, fingerprints, iris image depending on the country of issuance), as well as a digitally signed file allowing to check the authenticity and integrity the chip's

21 <https://www.passport-collector.com/league-of-nations-passport-conferences/>

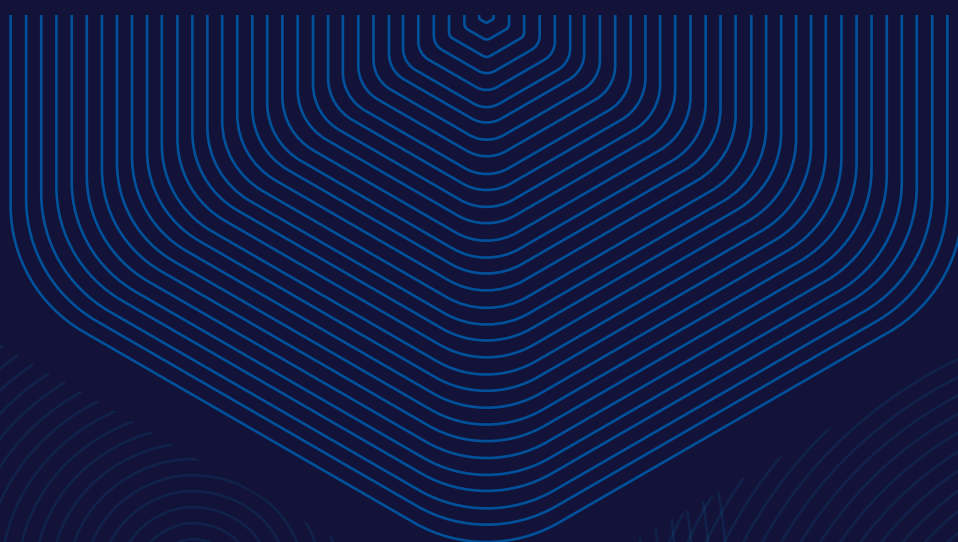
22 Turack, D.C., 1968. Freedom of movement and the international regime of passports. Osgoode Hall LJ, 6, p.230.

23 Machine-Readable Zone (MRZ) (https://idenfy.com/nitropack_static/GUBskGLjniYOsPEKytIvagiHcS-cYWiGq/assets/images/optimized/rev-091e626/www.idenfy.com/wp-content/uploads/2020/09/mrz-1.png)

24 Machine Readable Travel Documents in line with the requirements set in the ICAO Document 9303.

2

IDENTITY MANAGEMENT IN THE EU AND THE ROLE OF eu-LISA



2. Identity management in the EU and the role of eu-LISA

2.1. Digital identity and digital identity wallets

Digitising identity is a relatively novel concept within the realm of cross-border travel, while it is far from new in the context of digital services. State-issued digital identity has been widely used for over two decades²⁸, and before that, digital identity management solutions have been widely used, for example, by financial service providers (e.g., banks) in order to enable access to internet banking systems as early as the mid-1990s.

A legal framework for digital identity in the online domain applicable EU-wide was introduced with the Regulation on electronic identification and trust services for electronic transactions – the eIDAS Regulation²⁹ – in 2014, and has been in force since 1 July 2016. The regulation sought to improve cross-border access to digital public and private services using electronic identification issued in one Member State and recognised in other Member States. So far, 19 countries (18 EU Member States and Norway) have notified national eID schemes under eIDAS³⁰. The eIDAS regulation ensures that citizens and businesses can use their eID issued in one Member State when using an eID-enabled digital service in another Member State. The eIDAS framework relies on national eID systems relying on different standards and technical implementations, which makes the framework relatively complex.



An EU legal framework for online digital identity was introduced with the eIDAS Regulation in 2014

Following the somewhat limited success of the eIDAS regulation in stimulating the widespread adoption of electronic identity in cross-border applications in the EU³¹, in late 2020, Commission President Ursula von der Leyen announced a new initiative to develop European digital identity. This initiative aimed at providing easier access to digital services across Europe, as well as ensuring greater control over how identity data is shared. Following this announcement,

28 For example, in Estonia, where digital identity has been in place since 2002 and has been widely used to access public and private online services, as well as in internet voting.

29 Regulation (EU) No 910/2014. OJ L 257, 28.8.2014, p. 73–114

30 The notification process refers to the selection, peer review and official addition of national eID schemes to the eIDAS Network. Notification ensures that the eID schemes connected to the eIDAS Network satisfy the conditions of quality and security set out by the eIDAS Regulation. As a general rule, all eID schemes connected to the eIDAS Network must be notified, although in some cases service providers may make use of non-notified eID schemes.

31 Report from the Commission to the European Parliament and the council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0290>

the Commission performed an evaluation, which led to the revision of the eIDAS Regulation. The evaluation, while recognising some of the benefits provided by the eIDAS Regulation (e.g., legal certainty in digital transactions), identified a number of issues that limited the impact of the eIDAS Regulation, in particular as regards the benefits to end users.

The evaluation pointed out the persistent differences across Member States in accepting of eID for the provision of digital services, as well as the inability of the initial eIDAS framework to follow the latest technological developments (e.g., compatibility with electronic ledgers). The reliance on national eID schemes, as well as the primary focus on enabling cross-border access to public services, limited the wider uptake of eIDAS, including by private service providers³².

Since the adoption of the eIDAS regulation, digitalisation has penetrated a wider scope of day-to-day activities in which people and businesses are engaged. This trend has been boosted by the COVID-19 pandemic, requiring service providers to speed-up the pace of digital transition and, with it, a demand for more flexible and user-centred service delivery. Some of the requirements imposed by the new paradigm of digital services, such as the ability to integrate different verifiable data and certificates or credentials of the end user, could not be met by the current eID and trust services framework established by the eIDAS Regulation. Therefore, in order to adapt the digital identity framework to the requirements of modern digital services, the Commission committed to revise the eIDAS regulation on the basis of the evaluation performed in 2020³³.

The Proposal for a Regulation amending the eIDAS Regulation was presented by the Commission in June 2021 and the Regulation establishing the European Digital Identity framework was adopted in April 2024³⁴. The key change within the scope of the proposed Regulation is the introduction of a new European Digital Identity Wallet. The digital wallet will be issued by Member State authorities and will be used to store digital credentials provided to every EU resident willing to use the service. These digital identity credentials can be used in cross-border context to access public and private services that rely on trusted and secure digital identity solutions, while enabling end users to exercise control over sharing their identity data necessary for the provision of a specific service. With eIDAS 2.0, significantly large online platforms³⁵ that require user authentication will also be required to accept EU Digital Identity Wallet for authentication. Although the primary focus of the EU Digital Identity Wallet is on the use of digital identity to access digital services, it can also be used for storing digital travel documents.

Integrating travel documents and biometrics into digital identity wallets is useful in the context of the digitalisation of travel and border-crossing processes. In the wake of

³² Ibid.

³³ Ibid.

³⁴ Regulation (EU) 2024/1883, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:281:FIN>

³⁵ E.g., Amazon, Meta platforms (Facebook, Instagram), Google.

the global pandemic, a number of countries as well as international organisations and institutions, initiated or accelerated work on digital identity for different purposes, including travel, migration and asylum. These initiatives include the work of international organisations, such as ICAO on Digital Travel Credentials (DTC), IATA One ID³⁶, UN Digital ID³⁷, and a wide range of projects aimed at digitising identity for travel, migration and asylum purposes, including piloting the application of digital ledger technologies (blockchain) for identity issuance in the context of asylum procedures³⁸.

Taking into account technological developments in the area of identity management, such as biometric recognition and digital travel credentials, the European Commission has adopted a proposal for a Regulation establishing an application for the electronic submission of data (EU Digital Travel application), in October 2024³⁹. To support the preparation of the legislative proposal, the European Commission funded two pilot projects aimed to test the implementation of the DTC in real-life Schengen border-crossing scenario. Some of these technologies, as well as pilots, are explored in more detail later in this report (see 3.1.1).



The development and implementation of digital identity solutions within the context of border and migration management has intensified since the pandemic

The development and implementation of digital identity solutions within the context of border and migration management has intensified since the pandemic, with the realisation that some risks related to the spread of diseases can be somewhat reduced by reducing the number of in-person interactions and replacing those with digital alternatives (e.g., self-service kiosks). In addition, the Regulation on the digitalisation of the visa procedure entered into force on 27 December 2023⁴⁰. It foresees the

development of an online application platform by 2028 to allow visa applicants to directly request a Schengen visa online, as well as a digital visa, stored in a centralised database of the Visa Information System. As a fall-back option, instead of the visa sticker currently in use, the proposed Regulation suggests using a cryptographically-signed 2D barcode. As an alternative to the cryptographically-signed 2D barcode, an attestation stored in the end-user's digital wallet could also be used, taking advantage of the widespread use of smartphones around the world.

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

37 <https://www.unicc.org/news/2020/11/13/un-digital-id-a-building-block-for-un-digital-cooperation/>

38 https://www.bamf.de/SharedDocs/Anlagen/EN/Digitalisierung/blockchain-whitepaper-2021.pdf?__blob=publicationFile&v=3

39 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047

40 Regulation (EU) 2023/2667, OJ L, 2023/2667, 07.12.2023

Considering the role eu-LISA plays in developing and managing IT systems used in integrated border management and seamless travel facilitation, it is essential that the Agency closely follows and is involved in the development of novel solutions for identity management that will potentially interact with the systems it manages.

2.2. eu-LISA large-scale IT systems and identity management

eu-LISA is a major player in identity management at the EU level, in particular in the areas of visa, asylum, migration, and internal security. eu-LISA currently operates three large-scale IT systems: the Schengen Information System (SIS), the European Asylum Dactyloscopy Database (Eurodac), and the Visa Information System (VIS). Each of these systems includes identity management functions for a specific business domain:

- Eurodac handles identity management functions in the area of asylum.
- SIS handles identity data in the field of border management and internal security within the Schengen area.
- In the VIS, identity data is managed within the scope of visa procedures and border management.

“ ***With the entry into force of the new Eurodac Regulation, Eurodac will increase its scope in terms of identity management*** ”

The implementation of the new systems, namely the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), and the interoperability architecture will be gradual as per the decisions of the Justice and Home Affairs Council. Similar to the existing systems, the new systems will also store identity-related

information and fall under the identity management system hosted by the Agency:

- The EES will contain identity and related data on all third-country nationals (TCNs) crossing the Schengen borders for short-stay visits.
- ETIAS will handle identity and related data on visa-exempt TCNs crossing the Schengen borders.
- ECRIS-TCN will handle identity and related data on TCNs with criminal convictions in the EU. A summary overview of the systems managed and developed by eu-LISA is provided in Annex 1.

With the entry into force of the new Eurodac Regulation⁴¹, and the accompanying

41 An agreement between the co-legislators was reached in December 2024.

regulations which are part of the Pact on Migration and Asylum⁴², Eurodac will increase its scope in terms of identity management⁴³. The new Eurodac Regulation⁴⁴ extends the current Eurodac from being a system storing only biometric data (fingerprints), to include a range of biographical information, identity and travel document data, additional biometrics (facial image), as well as additional business information (see Table 1 for detailed overview). This will constitute a case management system, that will facilitate the identification of persons lodging multiple asylum applications in different Member States, and therefore help define the Member State responsible, as well as facilitate the handling and exchange of data and ultimately speed up the asylum process. In addition, this will help in tracing secondary movements of asylum seekers within the Schengen area. Furthermore, the new Eurodac will also support the implementation of resettlement schemes.

eu-LISA's identity management framework includes the following:

- Processes for creating, updating and removing identity data of individuals.
- Processes for verifying identities or identifying individuals.
- Policies, technologies, access rights and security measures.

In the context of the systems managed by the Agency, three types of identity-related data are being stored and processed by eu-LISA systems and Member State authorities:

- Biographical or alphanumeric identity data (such as first name, family name, date of birth).
- Biometric identity data (fingerprints and facial images, as well as templates).
- Associated business data (e.g., visas, passports, identity cards, travel file information, asylum requests, alerts, convictions, etc., in line with the business requirements of specific systems).

Currently, in the systems in operation (i.e., SIS, VIS and Eurodac), all data, including identity-related data, are handled within the tight constraints of the regulation of each individual system. Such a silo-based approach simplifies identity management and compliance with data protection requirements, as data is handled within an individual system and business domain. However, it does not provide the possibility to perform identification and verification across systems using a single search query. In addition to the inability to search all systems with a single request, requiring authorities to carry out parallel searches in each system, there are additional challenges whenever authorities need to search several systems independently as part of the same procedure:

42 https://home-affairs.ec.europa.eu/policies/migration-and-asylum/new-pact-migration-and-asylum_en

43 Currently Eurodac stores fingerprints of asylum applicants as a reference to an asylum application without any biographical data. Eurodac also stores fingerprints of people apprehended in connection with the irregular crossing of a Schengen external border.

44 Screening Regulation: Regulation (EU) 2024/1352 OJ L, 2024/1352, 22.5.2024

- Similar search requests need to be processed by dissimilar systems, to ensure consistency.
- These different systems need to process the search requests in consistent manner.
- The outcome of the comparison of the results (identity de-duplication process) is dependant on these two conditions

To overcome these challenges, and to simplify the tasks of the border guards and law enforcement officers using the systems, in 2017 the EU co-legislators approved the implementation of the Interoperability Architecture and its components: a single entry point, the European Search Portal, the Central Identity Repository, the shared Biometric Matching System, and the Multiple Identity Detector. The components, described in more detail below (see [2.3](#)), will act as bridges between the different systems. Searching identity information using biographic or biometric data for verification or identification purposes will become possible, and the identity de-duplication process will become easier and more robust, to support the detection of identity fraud.

2.3. Interoperability architecture and components

The main aims of the Interoperability Architecture are:

- To ensure that end-users, such as border guards, have controlled, fast, and seamless access to information relevant to business processes used for border control, visa issuance, assessment of asylum applications, law enforcement, etc.
- To detect multiple identities and potential identity fraud across all interoperable JHA information systems⁴⁵.
- To facilitate identity checks of third-country nationals.
- To facilitate, streamline and control access by law enforcement authorities to the information systems operated by eu-LISA.

The interoperability architecture is composed of the following components:

- The European Search Portal (ESP), will serve as a single access window to simultaneously query all systems operated by eu-LISA, as well as Europol and Interpol databases. It will provide access to identity data through profiles.
- The Common Identity Repository (CIR), will store identity-related data from all core business systems (CBSs), and will create individual identity files and support the multiple identity detection (MID) process.
- The Multiple-Identity Detector (MID), will create and store identity confirmation files

⁴⁵ Not all information systems developed and managed by eu-LISA are or will be interoperable. For example, the Joint Investigation Teams Collaboration Platform will operate separately from the interoperability architecture.

as well as establish links between identities, and allow their manipulation by end-users (i.e., border guards, law enforcement, etc.).

- The shared Biometric Matching Service (sBMS), will store biometric templates created from the biometric data stored in the CIR, to allow biometric matching functionalities, and enables querying on the basis of biometrics across the various CBSs.

Although on the one hand, the introduction of interoperability across the systems will increase significantly the complexity of identity management, on the other hand, individual components of the interoperability architecture, such as the sBMS, the CIR and the MID will simplify identity management and access to identity information by relevant authorities.

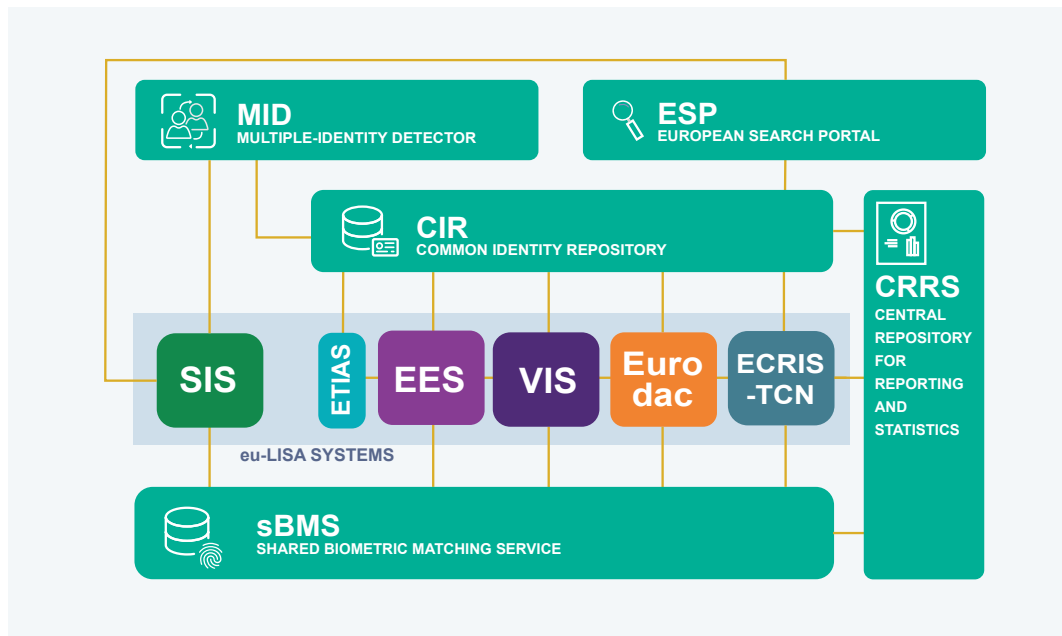


Figure 4: The JHA systems interoperability architecture

Identity deduplication process with the interoperability

The process of identity deduplication is necessary to ensure that identity information of the same individual captured under different circumstances when stored in the system(s) multiple times is connected to the previous record on the same individual (e.g., application file in the VIS or individual file in the EES). Each system processes identity deduplication when it captures and stores new data; the outcome of the process is a decision on whether newly captured identity data belongs to an individual already recorded in the system or not.

Before the interoperability architecture is in place, when querying multiple systems (e.g., VIS, SIS), identity deduplication needs to be done manually for every result received. Therefore, the more systems are queried simultaneously, the more identity deduplication procedures need to be carried out. In addition, differences between the search parameters (e.g., same attribute with different values – surname, last name or family name) affect the results from each system. This results in a time-consuming process for the end-users.

In performing the deduplication process, the MID is supported by the shared Biometric Matching Service (sBMS), by the Common Identity Repository (the CIR), and by the UMF (Universal Message Format) standard.

To ensure that the deduplication process works effectively, consistency of data is key. Currently, each CBS stores a mix of business and identity data. Identity data is needed to carry out the deduplication process. Consistency is achieved through centralisation of the processing of identity data in one system - the CIR. The CIR will provide a consistent approach to storing identity data, including travel document data, biometric data and biographic data (except for the SIS, which will still store identity data independently).

The sBMS ensures a fully standardised approach to handling biometric data, given that both SIS and CIR rely on the sBMS for processing of biometric queries.

The UMF standard enhances consistency across the systems (i.e., the CIR and the SIS), by ensuring that similar concepts are expressed in a consistent and semantically equivalent manner.

TYPES OF IDENTITY-RELATED DATA



Biographical or alphanumeric identity data (such as first name, family name, date of birth)



Biometric identity data (fingerprints and facial images, as well as templates)



Associated business data (e.g., visas, passports, identity cards, travel file information, asylum requests, alerts, convictions, etc., in line with the business requirements of specific systems).

IDENTITY DEDUPLICATION WITH INTEROPERABILITY

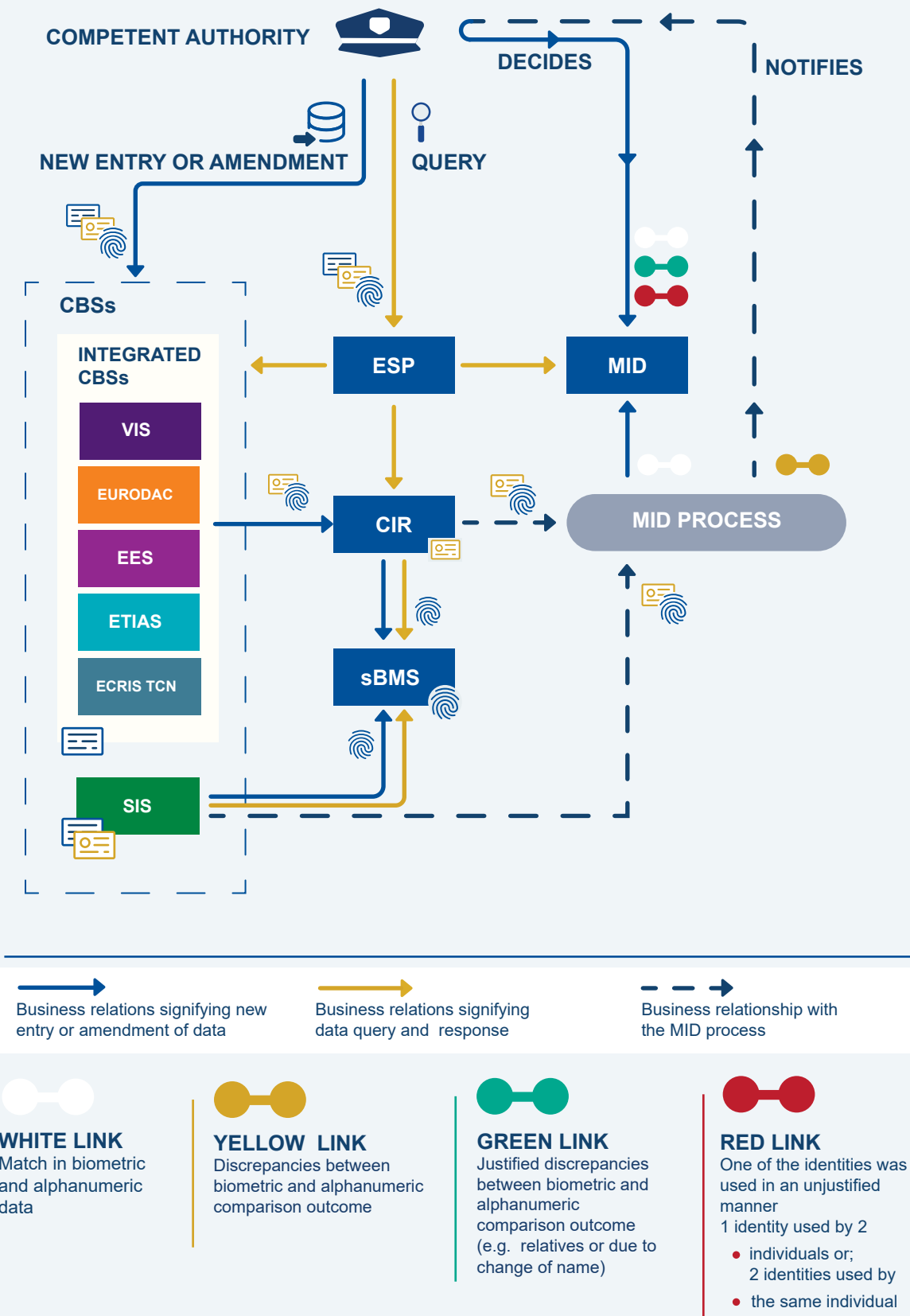


Figure 5: Identity deduplication process with interoperability

Table 1: Identity and identity-related business data stored in the large-scale IT system⁴⁵



VIS⁴⁶

Alphanumeric data on the applicant:

Surname(s)
First name/name(s)
Date of birth
Sex
Surname at birth (former surname)
Current nationality
Nationality at birth
Type and number of the travel document(s)
Date of expiry of the travel document(s)
Authority which issued the travel document(s) and date of issue.

Biometric data:

Photograph (face)
Fingerprints.



SIS⁴⁷

Alerts which include information on persons may contain the following alphanumeric data:

Surname(s)
First name(s)
Names at birth
Previously used names and aliases
Any specific, objective, physical characteristics not subject to change
Place of birth
Date of birth
Gender
Any nationalities held
The category, country of issue, number, date of issue, of the person's identification documents
A copy of the identification documents.

Biometric data:

Photographs/facial images
Dactyloscopic data (fingerprints).



EURODAC⁴⁸

Alphanumeric data

Sex

Biometric data

Fingerprints

Eurodac recast⁴⁹

Alphanumeric data

Surname(s)
Name(s)
Date of birth
Sex
Nationality
Date and place of application for international protection
Country of issue, type, number and expiry date of identity or travel document, as well as a scanned copy of the document
Visa application number and issuing MS.

Biometric data:

Fingerprints
Facial image.



EES⁵⁰

Alphanumeric data on TCNs crossing the border:

Surname(s)
First name(s)
Date of birth
Nationality (ies)
Sex
Type, number, date of expiry of the validity of the travel document(s)

Biometric data

Facial image
Fingerprints.



ETIAS⁵¹

Alphanumeric data of the applicant:

Surname(s)
First name(s)
Surname at birth
Date and place of birth
Country of birth
Sex
Current and other nationalities
First name(s) of the parents of the applicant
Other names(alias(es), artistic names, usual name(s))
Type, number, country of issue of the travel document

Date of issue and expiry of the travel document;
applicant's home address
Email address
Phone number
Education (level)
Current occupation (job group)
For minors: information about the person exercising parental authority or of the applicant's legal guardian
Application about family members residing in the Schengen area (when applicable).



ECRIS-TCN⁵²

Alphanumeric data:

Surname(s)
First name(s)
Date and place of birth
Nationality (ies)
Gender
Previous names
Parent's names
Identity number
Type and number of identity document, name of the issuing authority
Pseudonyms and aliases.

Biometric data:

Fingerprints
Facial images

45 Information valid at the date of the publication

46 Regulation (EC) No 767/2008, OJ L 218, 13.8.2008, p. 60–81

47 Regulation (EU) 2018/1860, OJ L 312, 7.12.2018, p. 1–13, Regulation (EU) 2018/1861, OJ L 312, 7.12.2018, p. 14–55 and Regulation (EU) 2018/1862, OJ L 312, 7.12.2018, p. 56–106

48 Regulation (EU) No 603/2013, OJ L 180, 29.6.2013, p. 1–30

49 Regulation (EU) 2024/1358, OJ L, 2024/1358, 22.5.2024

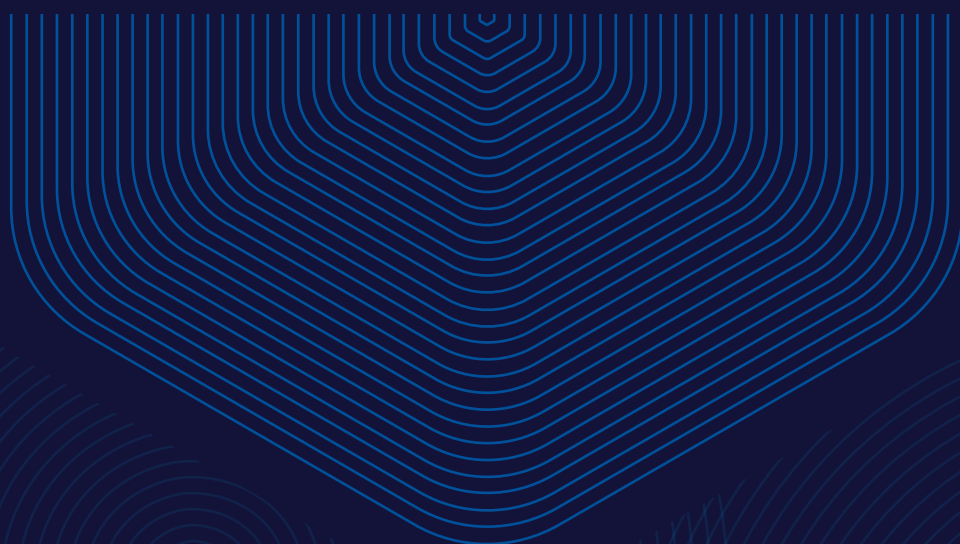
50 Regulation (EU) 2017/2226, OJ L 327, 9.12.2017, p. 20–82

51 Regulation (EU) 2018/1240, OJ L 236, 19.9.2018, p. 1–71

52 Regulation (EU) 2019/816, OJ L 135, 22.5.2019, p. 1–26

3

IDENTITY MANAGEMENT TECHNOLOGIES FOR CROSS-BORDER TRAVEL



3. Identity management technologies for cross-border travel

3.1. Remote enrolment of identity information

With the upcoming entry into operation of the Entry/Exit System, the busiest Schengen border-crossing points will likely face the challenge of enrolling third-country nationals into the EES, including their biometrics. Although modern technologies increase the speed of enrolment high-quality biometrics, this will nevertheless require additional processing time. This issue may become particularly acute during peak travel season, especially at land and sea border crossing points (BCPs) where existing infrastructure may not be suitable for installing a large number of self-service kiosks for individual enrolment in the system.

This challenge can be solved in at least two ways:

One approach is to install self-enrolment kiosks in the countries of origin, where travellers can pre-enrol their information (including biometrics) in a controlled environment in advance of their travel. Such approach will be used for passengers boarding Eurostar train in the UK, as well as travellers travelling from the UK using Eurotunnel, in which case enrolment of data into the EES will be done at the point of departure and not at a Schengen border-crossing point. Such practice of juxtaposed border controls for routes crossing the English Channel, based on reciprocal arrangements between Belgium, France, the Netherlands and the UK predates the introduction of the EES.

The main advantage of installing self-enrolment kiosks in the countries of origin of third-country nationals (TCNs) is to allow the capture and pre-enrolment of biometric information under supervision⁵⁴ and in controlled conditions in advance of travel. This will ensure high quality biometric data are collected, alleviating the burden of capturing them at Schengen BCPs. This could also be done through external service providers as the case for the processing of visa applications⁵⁵. This may significantly reduce the processing time at border-crossing points for TCNs travelling for the first time after the entry into operation of the EES or for TCNs who need to update their information in the EES. In addition, capturing biometrics in controlled conditions, could help ensure the capture of high-quality biometric data, as well as reduce the risk of identity fraud (e.g., presentation attacks). However, the investments required to install such equipment and make it available and easily accessible to TCNs would be disproportionate to the potential benefits gained, even if self-service kiosks are installed only in the countries/regions from where come the majority of TCNs travelling to the Schengen area.

⁵⁴ In the countries of origin, supervision shall be performed by officers of the country of destination, as is performed in the UK by the French and the Dutch authorities respectively.

⁵⁵ Such change would require amending relevant regulation(s).

Another approach is to allow travellers to pre-enrol their information in un-controlled conditions using, for example, mobile devices. In this scenario, no significant additional investments in infrastructure are required. Instead, consumer grade devices (smartphones with cameras and NFC readers) widely used around the world are used, thus making it a far more feasible solution to address the challenge of remote enrolment.

There are different ways of providing the necessary biometric and biographic information in a pre-enrolment scenario using a mobile device:

- One way is to use the information stored in a Digital Travel Credential (DTC);
- alternatively, biometric data can be captured using end-user devices.

Section 3.1.1 and 3.1.3 below provide a brief overview of both approaches.

3.1.1. Digital Travel Credentials

The ICAO Digital Travel Credential (DTC) concept was designed with the aim to facilitate travel through the creation of a secure and globally interoperable digital companion of the eMRTD (electronic machine-readable travel document) or to replace it. Similar to the use of machine-readable travel documents, issued according to a global standard, the standardisation of the digital representation of travel documents is essential to ensure their widespread adoption and acceptance by government authorities, as well as private operators (e.g., airlines). The security of the DTC issued according to the ICAO specification is ensured through a combination of physical and digital security features, which consist of:

- the DTC Virtual Component and
- the DTC Physical Component.

The DTC Virtual Component (DTC-VC) is the digital copy of the eMRTD, digitally signed by the issuing authority. In order to assure authenticity of the DTC, verifiers check the digital signature.

The DTC Physical Component (DTC-PC) carries the DTC-VC and serves as a physical authenticator through a cryptographic link created between the DTC-PC and DTC-VC; hence, only one DTC physical component is possible for each DTC virtual component.

In line with the ICAO Guiding Core Principles for the DTC⁵⁶, the DTC can be implemented in three different ways:

- Type 1 DTC – DTC bound to an electronic Machine-Readable Travel Document

⁵⁶ <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>

(eMRTD). Biometric and biographic information is read from an existing travel document (eMRTD) by the end-user and the eMRTD booklet (e.g., passport) is used as the authenticator of the virtual component. In this case, carrying a valid eMRTD is necessary.

- Type 2 DTC – DTC bound to a physical device and eMRTD. The DTC is created by reading the information from a valid eMRTD and cryptographically linked to another physical device (e.g., digital wallet on a smartphone). Such DTC can only be issued by the authority issuing eMRTD at any point in time after its issuance. The eMRTD serves as a fallback option.
- Type 3 DTC – DTC is issued by the authority issuing the identity documents (e.g., eMRTD), but a physical booklet is not issued. The DTC is cryptographically bound to a physical component (e.g., a digital wallet on a smartphone device).

In comparison to an RFID⁵⁷ chip on a passport, which has limited storage capacity, a DTC allows to store higher resolution images, in addition to the images downloaded from the eMRTD. Higher resolution images allow to comply with the requirements of the EES for the quality of facial images, and therefore also improve the performance of facial recognition systems.




	DTC TYPE 1 Self-derived	DTC TYPE 2 Authority derived	DTC TYPE 3 Authority issued
			
Issuance procedure	Generated by the holder by scanning a passport	Generated by the authority. Holder presents a passport in person	Generated by the authority either remotely or in-person. No passport required.
Physical component	eMRTD	Mobile device and eMRTD	Mobile device (temporary emergency document)
Virtual component	Mobile device /cloud	Mobile device /cloud	Mobile device /cloud
Usage for identification at BCPs	Passport is required	Passport is for reference purposes only	Smartphone only
DTC uses	Part of the border crossing procedure can be performed using a mobile device and biometrics; however, passport needs to be shown at least once, for example, at border control.	Only mobile device or biometrics are used by the traveller to prove their identity at all touchpoints.	Can be used only for emergency documents, in which case the traveller may present only their smartphone or biometrics to prove their identity.

Figure 6: Three types of Digital Travel Credential (DTC) as proposed by ICAO

57 Radio Frequency Identification

3.1.2. The EU Digital Travel Application – proposal for a Regulation

Following in the footsteps of ICAO, in October 2024, the European Commission proposed a Regulation establishing an application for electronic submission of travel data (i.e., the EU Digital Travel application)⁵⁸. The proposal aims to tackle the dual objectives of border security and facilitation of border crossing for legitimate travellers, considering the consistent growth in the number of travellers crossing borders and increasing complexity of processes at BCPs, since the entry into force of the Regulation (EU) 2017/458⁵⁹ on reinforcing checks at external borders, and the upcoming introduction of the EES in 2025. Today, border checks can only be performed once the traveller arrives at a Schengen BCP and presents a physical document for verification. Authorities are unable to verify the validity and authenticity of a travel document in advance (with the exception of visa holders). Furthermore, today, border authorities are unable to verify in advance whether third-country nationals fulfil entry conditions. These challenges are further exacerbated by the different levels of digitalisation of border procedures across the EU and Schengen Member States.

Challenges also exist for carriers operating across the Schengen border, who are responsible for the verification of identity, inspection of travel documents, as well as the consultation of relevant databases essential for security, but which contribute to the increase of traveller processing times, thus affecting the overall travel experience.

The proposed Regulation aims to address these challenges by:

- Setting a uniform standard for digital travel credentials for use in the context of Schengen border crossing.
- Establishing a common EU Digital Travel application.
- Allowing travellers (both EU citizens and TCNs) to use digital travel credentials to cross borders.
- Enabling border authorities to carry out advance checks against relevant databases on the basis of the digital travel credentials.

Enabling border authorities to perform advance checks will be key for travel facilitation, potentially resulting in a significant reduction of bottlenecks at the most active BCPs, as well as allowing to re-direct some of the freed human resources towards more critical tasks to ensure the more effective detection of cross-border crime and irregular migration.

⁵⁸ COM (2024) 670 final

⁵⁹ Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders (OJ L 74, 18.3.2017, p. 1)

One of the advantages of the implementation of the DTCs for border checks is that it is compatible with other existing or upcoming instruments targeted at enhancing border security and facilitating cross-border travel. Possible use cases⁶⁰:

- In the context of the **future digitalisation of visa procedure**⁶¹, a visa applicant could use the DTC to pre-fill information when submitting a visa application, while competent authorities could use the DTC submitted ahead of arrival to verify whether an individual has a valid visa.
- Similarly, in the context of the **ETIAS pre-authorisation of travel**, applicants could use a DTC to pre-fill information, while the border authorities could remotely verify that the person has a valid travel document.
- In the context of the EES, the DTC could be used to **remotely pre-enrol some of the travel data needed for the EES**, which, in combination with a remote acquisition of facial biometrics, would significantly reduce processing times at BCPs.
- Finally, in the context of the proposed Regulation on **advance passenger information (API)**, carriers could use the DTC to collect travel document data they are mandated to collect, in an automated way, which will result in more efficiency, as well as more accurate and reliable data.

The proposed EU Digital Travel application comes very timely, following the adoption of the eIDAS 2.0 Regulation, which established the concept of the EU Digital Identity Wallet (**see 3.3 below**). This paves the way towards a more widespread adoption of digital identification solutions in the EU, creating a fertile ground for the adoption of the DTC as a reliable and convenient means of identification in the context of cross-border travel, as well as in other scenarios, where DTC will be accepted as a means of identity verification by private or public sector service providers.

The high-level architecture of the EU Digital Travel application (hereinafter 'application') includes the following components:

- A mobile application available for installing on end-user devices.
- A validation service operating on centralised infrastructure that can verify the authenticity and integrity of travel documents, as well as the identity of the person using the application by comparing the facial image acquired using the end-user device with the image stored on the chip of the eMRTD.
- A centralised component ensuring secure transmission of traveller data between the application and the receiving authority, or the so-called Traveller Router.

The proposed Regulation establishing the EU Digital Travel application foresees the possibility for travellers to create DTCs for single or multiple use or to retrieve an already

60 COM(2024) 670 final

61 Regulation (EU) 2023/2667, OJ L, 2023/2667, 7.12.2023

created DTC, and to allow to store the multiple-use DTC in the EU Digital Identity Wallet⁶². According to the proposed Regulation, eu-LISA will be responsible for the development and maintenance of the mobile application and the Traveller Router, while Member States authorities will be responsible for setting up a secure connection to transmit traveller data to the national systems.

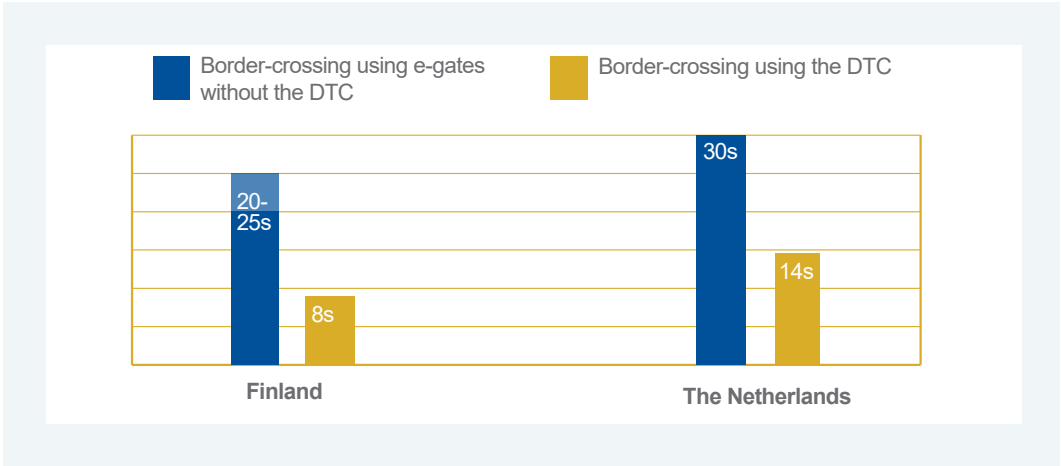
To support the impact assessment accompanying the proposed Regulation, the Commission supported two pilot projects that aimed to test the effectiveness of the DTC as a means to enhance border security and facilitation of traveller processing. Both pilot projects are described briefly in the box below.

European DTC Pilots

The DTC pilot projects were carried out by the Finnish, Croatian and Dutch authorities and supported by the European Commission. They had the following objectives:

- Explore how DTC can facilitate travel experience while ensuring high levels of security and respect for fundamental rights, including the protection of personal data.
- Contribute to the impact assessment supporting the legislative proposal prepared by the European Commission.
- Assess under what conditions the DTC and biometric boarding can be used in border control and passenger processing in compliance with the applicable regulatory framework.
- Gain a better understanding and experience with pre-verification of information submitted with the help of a DTC, passenger pre-screening and risk assessment.

The results of both pilot projects demonstrated that using the DTC in combination with e-gates can significantly improve border-crossing times, as shown in the table below.



62 OJ L, 2024/1183, 30.4.2024



DTC pilot – Finland⁶³

Completed in Q1 2024, the DTC pilot project in Finland was carried out in collaboration between the Finnish Border Guard, Finnair, the Finnish Police and Finavia at Helsinki Airport. The DTC pilot project allowed to facilitate the border control process for eligible passengers on Finnair flights, travelling outside of the Schengen Area. The pilot project implemented the DTC in a real border-crossing environment at Helsinki Vantaa airport. The solution developed within the project included the following components:

- A digital identity wallet with the ability to import a DTC and submit it in advance of travel.
- A kiosk for enrolling participants with pseudonymised personal data, to ensure compliance with the GDPR.
- A web portal for advance submission of the DTC.
- A system for DTC inspection at BCPs, including facial biometric matching and passport clone detection capabilities⁶⁴.

In addition to border checks, Finland piloted the use of the DTC in the context of residence permit issuance by the Finnish Immigration Service, in order to:

- Define requirements for setting up a digital residence permit.
- Define requirements for facial biometrics that are encodable in a digitally signed 2D barcode, and sufficient for visual identification.
- Develop a software app to verify the 2D barcode.
- Create technical specifications based on the outcomes of the pilot⁶⁵.

The pilot project relied on the following process:

Step 1: The traveller downloads and installs the DTC Pilot application on their smartphone.

Step 2: The traveller registers as a participant in the pilot at a police station. During the registration process, the passport is read, a photo is taken, a DTC is created in the Pilot app, and the end-user is asked to sign a consent form.

⁶³ Although the pilot project was carried out by the Finnish and Croatia authorities, here we focus on the Finnish pilot as integration between the systems in Finland and Croatia was not carried out, resulting in two separate and rather similar pilots.

⁶⁴ SWD(2024) 671 final – Impact Assessment Report accompanying the Proposal for a Regulation establishing an application for the electronic submission of travel data (“EU Digital Travel application”).

⁶⁵ Interim report of the Finnish and Croatian DTC pilot project.

Step 3: From 4 to 36 hours in advance of boarding an eligible flight, the traveller shares the DTC with the Finnish Border Guard using the app.

Step 4: At a border crossing point, the traveller presents themselves at a dedicated DTC-enabled e-gate. The DTC information is retrieved using the facial image. The traveller can then cross the border by tapping an NFC-enabled eMRTD (i.e. passport)⁶⁶.

The pilot was initially launched on Finnair flights to London, Manchester and Edinburgh, and was later expanded to all extra-Schengen Finnair flights. The results of the pilot project in terms of facilitation of border checks using the DTC were very positive. The average time for processing a passenger crossing border with a DTC was eight seconds, compared to the average time for EU citizens using e-gates of approximately 20-25 seconds, and in case of manual checks around 30 seconds. This time could be further reduced by automating some of the manual steps performed by border guards, as the actual facial recognition and chip authentication protocol can be executed by the system in two seconds.⁶⁷



Figure 7: Finnish DTC pilot⁶⁸ - Step 4

66 <https://raja.fi/en/dtc>

67 Interim report of the Finnish and Croatian DTC pilot project.

68 <https://raja.fi/en/dtc>



DTC pilot project – the Netherlands⁶⁹

The DTC pilot project in the Netherlands was carried out in collaboration between several public (i.e., the Ministry of Justice and Security, the Ministry of Interior and Kingdom Relations, the Ministry of Defence) and private (i.e., Idemia, Schiphol, KLM) actors. The pilot project was implemented on KLM flights between Canada and the Netherlands, and was available for participation of holders of Dutch, Belgian and Canadian passports. Similar to the Finnish pilot project, the pilot project in the Netherlands focused on testing the DTC Type 1 credential, which requires that the traveller carries a valid passport along with the DTC stored on a smartphone.⁷⁰

The pilot project relied on the following process (Figure 8)⁷¹:

Step 1: KLM sends an invitation to register for the pilot project to all eligible passengers on flights between Canada and the Netherlands (no visa required).

Step 2: Passengers interested to participate in the pilot project download a dedicated app, enroll for the pilot and create a DTC type 1 credential, by reading the RFID chip in the passport, and match the photo stored on the passport chip with a selfie.

Step 3: Passengers enroll into the pilot boarding process in the app and prepare for boarding by sharing the DTC with KLM to facilitate the boarding on a KLM flight to Schiphol.

Step 4: Passengers prepare for border crossing by sharing the DTC with the Dutch border authorities in advance of departure. Dutch border authorities carry out pre-assessment of the DTC and provide a digitised entry questionnaire to the passenger.

Step 5: Upon arrival at the border-crossing point, the passengers use dedicated DTC lanes. The pre-submitted DTC is retrieved using a facial scan, and the passenger can cross the border using the automated gate by reading the RFID chip of the passport.

The architecture of the Dutch pilot consisted of the following components:

- A DTC end-user application. A native iOS and Android application capable of using the NFC reader of the smartphone.

⁶⁹ A brief explanation of the pilot is also available in the following video: https://youtu.be/_eAywv_A4kw

⁷⁰ <https://www.government.nl/documents/publications/2023/02/23/dtc>

⁷¹ Adapted from: <https://www.government.nl/documents/publications/2023/02/23/dtc>

- A back-end system to verify the integrity and authenticity of passport data sent when creating the DTC.
- A boarding enrolment web-app.
- The KLM application used to verify the DTC prior to boarding, including the transmission of the DTC to the boarding gate.
- The integration of the boarding gate with biometric and eMRTD reading capabilities.
- A border-crossing enrolment web-app for enrolment of Canadian travellers.
- A Dutch border-control application, which checks the DTC for integrity and authenticity and enrolls the traveller in the pre-assessment application and in the border gates.
- A pre-assessment application available to the Targetting Centre Borders, responsible for advance checks.
- Border gates integrating facial recognition and NFC passport reading capabilities.

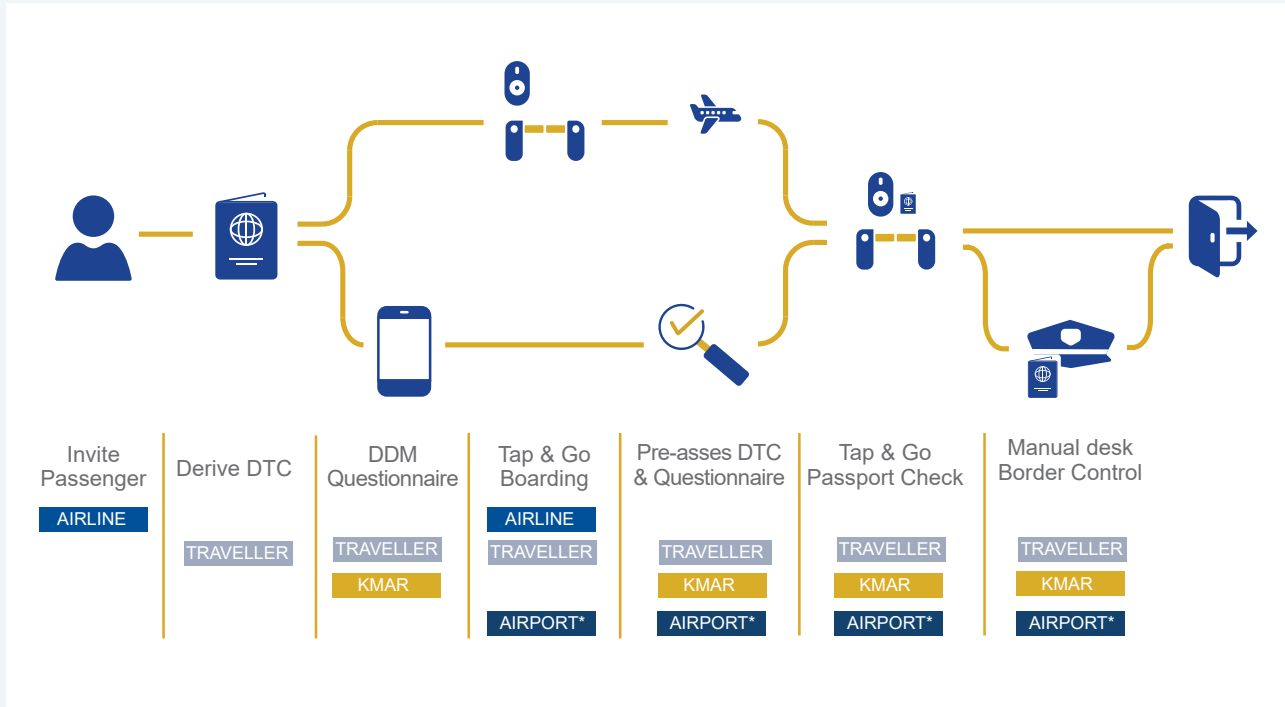


Figure 8: Dutch DTC Type 1 pilot project - Workflow process

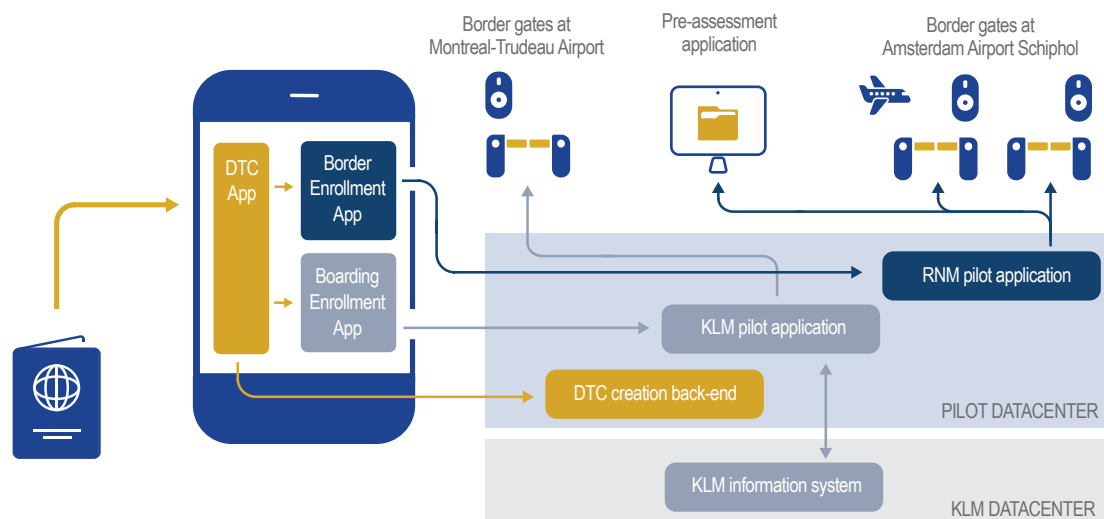


Figure 9: Dutch DTC Type 1 pilot project - Architecture⁷²

The Dutch pilot project highlighted a number of legal challenges, such as the requirement for a physical inspection of travel documents⁷², later addressed in the proposed Regulation for the EU Digital Travel application. Despite the challenges, the pilot project carried out in the Netherlands resulted in a number of positive outcomes:

- The pilot project has proven that the use of DTC in border management processes facilitates identity verification and speeds up traveller processing.
- Implementing digitised entry questionnaires has also contributed to the improved efficiency (90% of travellers offered the option, uses it).
- The time needed for border crossing procedure using the DTC is ca half compared to the current e-gates (14 vs 30 seconds per passenger).⁷³

⁷² For a full list of legal challenges see pp.19-20 of the final evaluation report of the Dutch DTC pilot available here: <https://www.tweedekamer.nl/downloads/document?id=2024D27941>

⁷³ The pilot also produced a number of operational, legal and technical recommendations, which are available on pp.38-41 idem.

3.1.3. Remote enrolment of identity data beyond the DTC: opportunities and challenges

Remote enrolment of identity information in the context of travel and border-crossing processes (e.g., pre-enrolment in the EES) does not necessarily require the creation of a DTC. An alternative way is to enrol all information (i.e., biographical and biometric) using a dedicated application. As a first step, the end-user captures the passport's data page with a smartphone camera, and then reads the RFID chip of the eMRTD (passport) with the NFC (near-field communication) reader embedded in their personal smartphone. The user then takes a selfie picture of their face, with some guidance regarding lighting and background, in order to ensure high quality of the facial image. Before enrolment, the captured selfie is compared with the image stored in the eMRTD chip, and the image printed on the passport page. This provides a certain level of confidence that the person enrolling their identity data is not an impostor.

Given that the number of fingerprints contained in the eMRTD is limited to two index fingers (in most cases), the enrolment of fingerprints needs to be done separately using devices compliant with requirements set in the Implementing Decision setting specifications of quality of fingerprints and facial images for the EES⁷⁴. At the moment, the requirements for fingerprint quality set in this act can only be met by FBI-certified touch-based fingerprint readers. Therefore, it is not possible to use end-user devices (smartphone cameras) to capture fingerprints for enrolment in the EES. Nevertheless, there are solutions addressing this challenge, albeit imperfect.

Over the past decade, with the improving quality of camera hardware and software embedded in smartphones, significant advancements have been made in the development of innovative solutions for the acquisition of fingerprints using smartphone cameras. In comparison with contact-based fingerprint scanners, contactless acquisition methods offer the following advantages:

- Less constraints in terms of capturing environment.
- Significant reduction of the effect of skin conditions (e.g., skin dryness).
- Absence of latent fingerprints⁷⁵ on the sensor.
- Improved hygiene.

When performed in controlled or semi-controlled conditions, contactless fingerprint acquisition demonstrates performance similar to touch-based fingerprint scanners⁷⁶. However, in uncontrolled conditions, the performance of contactless acquisition with a smartphone camera is much less reliable. For example:

⁷⁴ Commission Implementing Decision (EU) 2019/329

⁷⁵ Fingerprints left by previous travellers

⁷⁶ Priesnitz, J., Huesmann, R., Rathgeb, C., Buchmann, N. and Busch, C., 2022. Mobile contactless fingerprint recognition: implementation, performance and usability aspects. *Sensors*, 22(3), p.792

- To capture high-quality sharp images suitable for further processing, camera focus needs to be very accurate and fast. In challenging lighting conditions, achieving sharp images with most devices available off the shelf today will be challenging.
- The acquisition of high-quality fingerprint images requires clear separation of hands/fingers from the background. To achieve best results, homogeneous background is beneficial, however it is difficult to achieve in uncontrolled settings⁷⁷.

These performance limitations in uncontrolled conditions do not yet allow to effectively use consumer grade devices (smartphones) for contactless acquisition of fingerprints either by end-users or border-guards operating in challenging conditions (e.g., performing their duties within coaches, trains, or ferries, or challenging weather conditions). Achieving robust acquisition of fingerprints using consumer grade devices requires additional steps, such as enhanced lighting and a stable platform to which the equipment used for acquisition can be affixed to ensure high-quality sharp images and therefore high quality of biometric samples.

In addition to the issue of quality of fingerprint images acquired using smartphone cameras, there is an issue of interoperability of fingerprints acquired using contactless techniques with fingerprints acquired using contact-based sensors. Recent research focusing on improving interoperability between contactless and contact-based fingerprints, which includes the development of models for distortion correction in contactless fingerprints, suggests that significant improvements in reducing error rates are possible⁷⁸. Despite these significant advances, contactless fingerprint acquisition technologies cannot be used for enrolment in the context of the EU large-scale IT systems, as they are not yet compliant with the relevant standards for fingerprint quality. However, considering the significant improvement in terms of performance of contactless systems, there is potential to deploy contactless fingerprint recognition using smartphone cameras embedded in end-user devices used by law enforcement authorities (LEAs) and border guards for authentication purposes, to allow for a more portable and easy-to-use equipment.

In some industries, remote identity verification using biometrics has already been implemented. For example, in the financial services industry, where customer identity verification is an essential component of know your customer (KYC) procedures put in place as part of measures tackling money laundering, remote identity verification has been used for some time by fintech start-ups who rely on online service delivery channels as a competitive advantage against traditional banking. Similarly, the UK government has implemented remote identity verification in the context of the EU settlement scheme introduced after the Brexit, in order to facilitate and speed-up the processing of applications for immigration status submitted by EEA nationals residing in the UK⁷⁹.

⁷⁷ Ibid.

⁷⁸ see Kauba et al., 2021. <https://www.mdpi.com/1424-8220/21/7/2248>, also Priesnitz, et al., 2022

⁷⁹ <https://www.inverid.com/use-cases/uk-home-office-euss>

The success of the implementation of remote identification technologies in terms of preventing identity fraud depends to a large extent on the way the remote enrolment process is done and what technologies are used in the back-end to tackle identity fraud, in particular focusing on the detection of fraudulent documents, as well as biometric attacks (see 3.1.4 below).

3.1.4. The risk of presentation attacks in the remote enrolment of biometrics

With the advancement of contactless fingerprint recognition technology, researchers have been dedicating more attention to the development of presentation attack detection (PAD) algorithms and systems, to ensure that contactless systems are well-protected against presentation attacks⁸⁰. In presentation attacks, an ill-intentioned individual uses an item (e.g., rubber fingertips, face mask) that mimics the biometric characteristic of the legitimate user to impersonate them and gain access to the system⁸¹. In 2023, the first competition on non-contact fingerprint-based PAD was held, to test algorithms and systems developed specifically for liveness detection in contactless fingerprints. Testing of PAD algorithms (for single fingerprint) and systems (for four fingerprints) was done using a variety of presentation attack instruments (PAI), including printed finger photo,

“ *In presentation attacks, an ill-intentioned individual uses an item (e.g. rubber fingerprint, face mask) that mimics the biometric characteristics of the legitimate user to impersonate them*

Ecoflex PAI, latex PAI, Playdoh PAI, wood glue PAI, synthetic (generated) fingertip PAI. The competition was open to all vendors; four submissions were assessed in the algorithms category and two submissions assessed in the systems category. The winning algorithm achieved an ACER⁸² of 6%, whereas the winning system in the systems competition achieved ACER of 7.36%, however, most of the algorithms performed poorly against synthetic fingertips (deepfakes) that they were not exposed to before. Further development of PAD techniques therefore is necessary to further improve their performance, in particular for contactless techniques.

80 See e.g., J. Priesnitz, R. Casula, J. Kolberg, M. Fang, A. Madhu, C. Rathgeb, G. Marcialis, N. Damer, C. Busch: “Mobile Contactless Fingerprint Presentation Attack Detection: Generalizability and Explainability”, in IEEE Transactions on Biometrics, Behavior, and Identity Science (TBIOM), (2024); J. Gonzalez-Soler, M. Gomez-Barrero, C. Busch: “Towards Generalisable

81 https://www.eulisa.europa.eu/sites/default/files/documents/eu-lisa_technology_brief_biometrics_part1.pdf

82 Average Classification Error Rate is a performance metric that takes into account both false positive and false negative errors and therefore provides a balanced assessment of the system’s ability to correctly classify both positive and negative instances.

When it comes to the remote enrolment of facial biometrics, most of the smartphones available on the market have cameras suitable for capturing facial images that meet the requirements of biometric recognition systems. Applications provided to end-users for enrolment of facial biometrics should guide end-users to ensure high image quality using specific prompts regarding even background or ambient lighting. Such applications should also include a face quality assessment tool, to ensure that the captured image meets quality requirements to be uploaded in the system. However, capturing a high-quality facial image using an end-user device addresses only part of the problem.

Aside from the quality of captured images, the main challenge in the remote enrolment of biometrics is the lack of trust and lack of ability to control the environment in which users perform enrolment, as well as the impossibility to control users' actions. This affects the capacity of authorities to determine whether the captured biometrics truly belong to the individual claiming a specific identity and can therefore be bound to the biographical information provided. Similar to fingerprint recognition, a number of attacks can be deployed by persons operating with criminal intent in an attempt to exploit face recognition systems, including presentation attacks, morphing attacks, as well as digital injection attacks.

Presentation attack is the simplest version of an attack, in which printed images, face masks, synthetic fingerprints, make-up or impersonators are used to interfere with the normal operation of the biometric system.



Figure 10: Morphed image of two US presidents is in the centre of this image⁸³

Morphing attack is a more complex attack, in which, a composite image of two persons is used to issue a legitimate passport. The synthetic composite image (see example above), which is very difficult to discern from a legitimate facial image even for trained experts, is positively matched by automatic recognition systems to the two individuals that provided their facial images to create the morphed image. The resulting passport

⁸³ <https://www.researchgate.net/publication/341882733/figure/fig1/AS:961398649659405@1606226708474/Morphing-between-the-original-faces-of-US-President-George-W-Bush-left-and-US.jpg>

using this image can then be used by the legitimate owner but also by the second person whose facial image was used to generate the synthetic composite image stored in the passport. This means that a person with criminal intent can use the passport to cross borders, as well as for remote enrolment using processes described above.

Digital injection attack is the most complex attack, during which camera of the end-user device is circumvented and a digital image is injected into the application instead of a selfie. Such attacks are much more scalable than presentation or morphing attacks, in particular in the age of generative artificial intelligence.

With the proliferation of the use of facial recognition across a variety of scenarios, including remote identity verification in the context of financial services, the need for the development of robust techniques for presentation attack detection (also referred to in literature as liveness detection) has also become more acute. Different approaches have been developed to ensure liveness detection in the context of remote biometric recognition and help tackle digital injection attacks:

- Some liveness detection techniques rely on motion tracking and require active cooperation of the subject⁸⁴.
- Other techniques rely on a specific sequence of coloured light projected on the subject's face using smartphone screen and then captured by a camera and verified by an algorithm⁸⁵.
- Some devices, such as Apple iPhone with an embedded infrared camera and an infrared LiDAR, in addition to using an image acquire in the visible spectrum, use depth perception to map a 3D representation of the face. This not only helps improve accuracy, but also protects from some presentation attacks (e.g., when a printed image is used). However, considering that such technology is available in less than 25% of smartphone devices worldwide, and that it addresses only some of the possible attacks, other solutions that would cover a larger share of end-user devices need to be considered.

Morphing attacks can be prevented by ensuring that images embedded in identity documents are taken in controlled conditions. However, this is not always feasible. Even in EU Member States which require that document photos are taken on premises of the document issuing authorities make exceptions in certain cases, for example, when an application for a new passport is submitted at an embassy. Allowing applicants to submit a passport photo made elsewhere, opens the document issuing system to the potential use of morphed images in legitimately acquired documents. Therefore, it is important to ensure that morphing attack detection algorithms are used in the remote pre-enrolment process or when processing travellers at border-crossing points (e.g., when enrolling TCNs into the EES). Considering the relative complexity of morphing attacks, those

84 See e.g. US Patent US10691934B2

85 See e.g. US Patent US9773180B2.

may not be as common; however, given that morphing attack detection tools may not be readily available to border guards, and human evaluators are not very effective in identifying morphed faces, the number of known morphing attacks may be significantly lower than the number of morphing attacks that have been carried out⁸⁶.

Remote pre-enrolment of some identity information in advance of travel or crossing the border has potential to reduce congestion at border crossing points. However, a careful assessment needs to be performed as to which identity information can be pre-enrolled remotely while limiting the risks that this false or fraudulent identity information may be entered in the central systems. Using some of the technologies outlined above may help reduce potential identity fraud, but those will not eliminate such fraud completely. Moreover, the use of personal devices for capture and enrolment of biometric data may be limited by the applicable legal requirements.

3.2. Solutions for fraud detection in identity documents

“ **Artificial intelligence has been effectively used to support immigration and asylum authorities in the detection of fraudulent identity documents**

One area where artificial intelligence has been effectively used to support immigration and asylum authorities is in the detection of fraudulent identity documents. Over time, the number of security features on document has increased significantly, and countries continue improving the security of travel documents with each iteration. Although this enhances document security, it has made it increasingly difficult, if not impossible, for human assessors to verify which of the security features should be present in a document and where

those should be located on a passport. As a result, authorities responsible for border management, visa issuance and asylum procedures have been increasingly looking towards technology to support them in assessing the veracity of documents. Over the years, the European Commission has funded a number of projects focusing on fraud detection in identity documents and biometrics more specifically, including two of the most recent ones – D4FLY and iMARS.

The recently completed D4FLY⁸⁷ Horizon 2020 project was dedicated to the development of a set of solutions targeted at the detection of fraud using automated tools, including artificial intelligence. Their suite of tools includes the following components⁸⁸:

86 For a comprehensive overview of morphing attack generation and detection techniques see Venkatesh et al., 2021 <https://ieeexplore.ieee.org/abstract/document/9380153>

87 Detecting document fraud and identity on the fly - <https://d4fly.eu/>

88 For more information see Bouma, H. et al. (2021) “Authentication of travel and breeder documents,” Proc. SPIE, vol. 11869, (2021). <https://doi.org/10.1117/12.2598143>

- A component for KINEGRAM⁸⁹ analysis, which is comprised of a set of checks performed across high-resolution images acquired from a document scanner using multiple light sources (visible, near infra-red and ultraviolet). The checks are performed against a template, focusing on the size and position of the KINEGRAM within the data page, on the shape of the KINEGRAM, on the colours and structures of the KINEGRAM, as well as other properties, such as texture, contrast, etc.
- Advanced Document Analysis Module, which uses computer vision algorithms to analyse specific document security features, such as Multiple Laser Images and Changeable Laser Images, which are not detected automatically by current current software.
- Analysis of printing techniques. Both travel and breeder⁹⁰ documents may contain different printing techniques (e.g., offset, inkjet, laser). In addition, documents often bear stamps and signatures. Analysing of printing techniques may assist in detection of forged documents, as forgeries tend to be created using alternative printing techniques than used for original documents.

Considering that breeder documents can be used in asylum and visa application procedures, tackling identity document fraud is essential, and the use of digital tools, including machine learning, may aid Member State authorities in addressing identity fraud more efficiently and effectively.

The currently ongoing iMARS⁹¹ Horizon 2020 project builds on the work of D4FLY on identity document fraud, with a focus on image manipulation, and in particular on image morphing. The iMARS project aims to:

- Develop an image manipulation and morphing detection software (TRL-6⁹²) that will improve the practitioners' fraud detection capacity.
- Develop efficient and mobile solutions for ID document verification, checking document validity, detecting and counteracting document fraud.
- Develop efficient face image quality assessment software that will predict recognition performance.
- Validate the iMARS solutions against operational requirements in emulated scenarios.

The iMARS project aims to develop two types of differential morphing attack detection: explicit and implicit. The former method includes explainable features such as texture descriptors or landmarks. The latter is mainly based on artificial neural networks and

⁸⁹ An optically variable mark used to prevent counterfeiting.

⁹⁰ Documents used to support applications for identity, residence or travel documents (e.g., visas), such as birth, marriage and death certificates.

⁹¹ Image manipulation attack resolving solutions - <https://imars-project.eu/>

⁹² Technology demonstrated in relevant environment. https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

deep learning. Following the development and testing of different individual methods, the project will also deploy fusion of the best-performing approaches to further improve performance of the morphing attack detection system overall. The tools will then be assessed using independent testing platforms at NIST⁹³ and BOEP⁹⁴.

3.3. Digital identity wallets and self-sovereign identity

With the growing need for identity verification online, there is a growing need for solutions that provide robust identity verification capabilities, while ensuring strong protection of personal data, which can be ensured through limited disclosure. As the digital landscape evolves, digital identity wallets (DIWs) are becoming essential tools for secure and user-centric identity management in various online interactions, from financial transactions to accessing digital services (**see also 2.1 above**). During the COVID-19 pandemic with the widespread use of vaccine certificates, wallets became a necessary solution to efficiently modernize identification systems. Government-issued wallets are a solution to streamline citizens' interactions for official purposes, such as e-signatures, identification, electronic transactions etc. These DIWs must ensure security for the storage and transition of sensitive data.



What is a digital identity wallet?

A digital identity wallet is a secure and electronic repository for managing and storing various aspects of an individual's digital identity. It serves as a virtual container for personal information, credentials, and authentication tokens, allowing users to control and share their identity data selectively. Digital identity wallets offer a convenient and safe solution to sharing verified information, from medical records and biometric data to memberships and loyalty cards.

One of the key concepts in the space of sensitive identity-related data and digital identity wallets is the concept of self-sovereign identity (SSI). SSI describes the right of an individual to have full control and ownership of their data and identity in the digital space, as they would offline. The principle is in its infancy, as there is no limit to the information that might be collected and put to use, from e-commerce transactions to data from social media accounts. However, when it comes to sensitive data such as biometrics, health information, and verifiable credentials, it is of fundamental importance to structure DIWs and Digital ID systems around SSI principles (see Table 2) – and made impervious to forgery, fraud, and data leakage. The Self-sovereign Identity system (SIS) is a two-party relationship, as it directly connects the user to the organization as a peer. In a SIS there are three entities: owner, issuer, and verifier. The 'issuer' (public or private organisation)

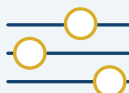
93 National Institute of Standards and Technology. See e.g. Face Analysis Technology Evaluation (FATE) Part 4: MORPH – performance of Automated Face Morph Detection https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf

94 Bologna Online Evaluation Platform: <https://biolab.csr.unibo.it/fvcongoing/UI/Form/BOEP.aspx>

Table 2: Principles of Self-Sovereign Identity⁹⁵



Existence - Users must have an independent existence. A self-sovereign identity is based on the ineffable “I” at the heart of identity, which cannot exist wholly in digital form. It makes limited aspects of the existing “I” public and accessible.



Control - Users must control their identities. They are the ultimate authority on their identity and should be able to refer to it, update it, or hide it. While other users may make claims, the user should control their identity, deciding between celebrity or privacy as they prefer.



Access - Users must have access to their own data. They should easily retrieve all claims and other data within their identity, with no hidden data or gatekeepers. This doesn't necessarily grant modification of all claims but ensures awareness of them. Users do not have equal access to others' data, only to their own.



Transparency - Systems and algorithms must be transparent. The systems used to administer identities must be open, both in function and management. Algorithms should be free, open-source, well-known, and independent of specific architectures, allowing anyone to examine their operations.



Persistence - Identities must be long-lived. Ideally, identities should last as long as the owner of identity is alive, or as long as the owner wishes. Private keys may need rotation, but the identity remains. A “right to be forgotten” is respected, allowing disposal of an identity if desired, with claims modified or removed over time.



Portability - Information and services about identity must be transportable. Identities should not be held by a singular third-party entity, ensuring user control despite potential entity disappearances or jurisdictional changes. Transportable identities improve persistence and autonomy over time.



Interoperability - Identities should be widely usable. The goal is to make identity information globally available, crossing international boundaries, without losing user control. Thanks to persistence and autonomy, widely available identities can become continually accessible.



Consent - Users must agree to the use of their identity. Sharing of identity and claims occurs with user consent, even if not interactive. Other users presenting claims require user consent for them to be valid, preserving deliberate and well-understood consent.



Minimalization - Disclosure of claims must be minimized. When data is disclosed, only the minimum necessary for the task should be revealed. Minimalization is supported by selective disclosure, range proofs, and zero-knowledge techniques to enhance privacy protection.



Protection - The rights of users must be protected. In conflicts between the identity network and individual rights, the network should prioritize preserving individual freedoms. Identity authentication should use independent, censorship-resistant, force-resilient, and decentralized algorithms.

⁹⁵ The Path to Self-Sovereign Identity, Allen C. available at: <https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md>

will issue Verifiable Credentials (VCs) to the ‘owner’ (individual) who will store it submit it to ‘verifiers’ (service providers) who rely on the integrity and authenticity of the credentials issued by trusted issuers⁹⁶. Specialized services, known as Identity and Access Management (IAM) systems are the trusted actors who handle the authentication processes⁹⁷. The identification process typically involves presenting a unique attribute (an identifier) in a specific context. For example, providing an email address during the sign-up process for a subscription service is a common practice. This method allows owners to only share a relevant information, in contrast to traditional physical or digital credentials, where the entire identity document must be disclosed, revealing all attributes⁹⁸.



COVID-19 certificates

Which provided proof of vaccination, test or recovery from COVID-19, were one of the early attempts to use identity-related credentials in a cross-border setting. The EU Digital COVID certificate has been a crucial element in Europe’s response to the COVID-19 pandemic, with more than 2.3 billion certificates issued. The certificate facilitated safe travel for citizens across the European Union when Member States restricted travel on the grounds of public health. In addition, it allowed to coordinate the lifting of these restrictions from the moment it was possible. In 2023, the WHO adopted the EU system of digital COVID-19 certification to establish a global system.

3.3.1. Blockchain for identity management and verification

Given the expansion of digital identity services, such as the EU Digital ID (EUID) for all citizens, there is a need for technologies that facilitate storage, access, and management of identity data through a Digital Identity Wallet. A significant challenge arises from the current highly fragmented digital identity landscape. One viable solution being explored for storage and encryption is the use of a Blockchain management system. Blockchain⁹⁹ is not a requirement for decentralised identity but it can provide a trustworthy

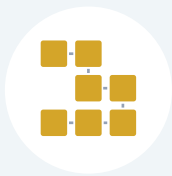
96 Islam, Md Tarekul & Hasan, Md Mahedi & Nasir, Mostofa & Gazi, Mohammad & Faruque, Golam & Hossain, & Azad, Dr. (2022). Blockchain-Based Decentralized Digital Self-Sovereign Identity Wallet for Secure Transaction **Blockchain-Based-Decentralized-Digital-Self-Sovereign-Identity-Wallet-for-Secure-Transaction.pdf** (researchgate.net).

97 Wang, Fennie and De Filippi, Primavera, Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, in *Frontiers in Blockchain* (Special Issue on Identity and Privacy Governance), 2020 , Available at **Frontiers | Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion** (frontiersin.org)

98 Schardong F, Custódio R. Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. *Sensors* (Basel). 2022 Jul 28;22(15):5641. doi: 10.3390/s22155641. Available at: **Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy - PMC** (nih.gov)

99 Ammous, S. (2016). Blockchain technology: What is it good for?. Available at: https://web.archive.org/web/20180921223508id_/http://www.ieepes.org:80/ee335/papers/SSRN-id2832751.pdf

decentralized management infrastructure for digital IDs with respect to SSI. The blockchain offers a viable option to ensure ID validation through a trusted authority and encrypted sharing, while the individual maintains full control¹⁰⁰; in blockchain based SSI systems there is less dependence on centralized authorities, and trust is instead shifted to a decentralized entity. There are many methods that can be used to achieve authentication, privacy and trust within the blockchain, such as uPort ShoCard, and Sovrin¹⁰¹. They differ in how data is shared with other parties, how personal identity is disclosed, front-end interface and usability etc. These options make it more or less appropriate to be used in the context of a national identity or an EU digital ID. A fundamental aspect of these functions is to ensure that only authorized individuals can access associated resources. However, all systems have some level of weakness and limitation, from their scalability and economic cost, to conflicting responsibilities and security threats¹⁰².



What is a blockchain?

Blockchain is a decentralized digital database relying on peer-to-peer data transactions, operates by grouping data into cryptographically secured blocks that are sequentially linked through a consensus mechanism. With a new block generated at regular intervals, the blockchain's structure is particularly difficult to compromise.

The blockchain is a powerful tool with a large application potential in the public sphere. This has spurred the European Union's active involvement in developing the European Blockchain Services Infrastructure (EBSI)¹⁰³. EBSI is a blockchain service infrastructure being built by and for the European Union, that functions as a foundational blockchain service infrastructure, providing a secure base for trusted functionalities like data sharing, digital identity management, and official notarization. Each member of the European Blockchain Partnership (EBP), EU27, Norway, Liechtenstein and the European Commission contributes by operating one or more nodes¹⁰⁴. The decentralized pan-European node distribution mitigates the risk of a single point of failure, presenting a resilient infrastructure distinct from conventional centralized models. The EBSI architectural pillars include accessible APIs for application connectivity on the public internet, Smart Contracts acting as intermediaries between external interfaces and the ledger, and a decentralized database facilitating information access for entities engaged in diverse business processes¹⁰⁵.

100 https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

101 Liu, Yang & He, Debiao & Obaidat, Mohammad & Kumar, Neeraj & Khan, Khurram & Choo, Kim-Kwang Raymond. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*. 166. 102731. 10.1016/j.jnca.2020.102731

102 Ibid.

103 <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home>

104 [European Blockchain Services Infrastructure | Shaping Europe's digital future \(europa.eu\)](#)

105 [What is EBSI - EBSI - \(europa.eu\)](#)

However, while offering certain advantages, using blockchain for identity management has its challenges.

- Blockchain networks, particularly those based on the proof-of-work consensus mechanisms, require significant computational power and comparatively slow transaction speeds, which makes them hard to scale.
- As mentioned above, identity data (including biometrics) is dynamic, which makes it challenging to reconcile with immutability of blockchain ledgers. In addition, due to immutability of records, blockchain is effectively non-compliant with the GDPR, which requires the possibility that personal data can be removed.
- Considering that the use of blockchain by public authorities would require the creation of a private permissioned blockchain network, operating such network may be costly.
- Finally, blockchain is still a relatively immature technology, which makes it less suitable for government applications which require high levels of stability, safety and reliability, in particular with highly-sensitive applications, such as identity management for asylum seekers and refugees.¹⁰⁶

3.3.2. Some examples of digital identity wallet implementations

To achieve the goal of having an integrated EU Digital Identity Wallet, four pilot projects have been funded by the European Commission to explore a variety of solutions and technologies. DC4EU stands out for the incorporation of EBSI and eIDAS at the core of the system. DC4EU will undertake extensive pilot programs to explore the deployment of a social security Wallet across all EU Member States. The technology will be based on the European Digital Identity Architecture and Reference Framework (ARF), which contains all the specifications needed to develop an interoperable EUDI Wallet Solution based on common standards and practices. The ARF was used to develop the EUDI Wallet reference implementation¹⁰⁷, which will be further developed on the basis of the results of several large-scale pilots funded by the Commission, which are briefly described below.

Although the primary focus of the eIDAS regulation is on the provisioning of identity and trust for digital services that are provided using the Internet, digital identity wallets will also be useful in the context of international travel, as they can store digital travel credentials. Such credentials can be used, for example, for providing identity information when submitting an ETIAS application, or when crossing a border. However, adoption of a single global standard for DTCs (or interoperable standards) will be necessary first, to ensure that solutions adopted by countries outside of the EU are compliant with the requirements.

¹⁰⁶ <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/758/wi-758.pdf>

¹⁰⁷ <https://github.com/eu-digital-identity-wallet/github/blob/main/profile/reference-implementation.md>

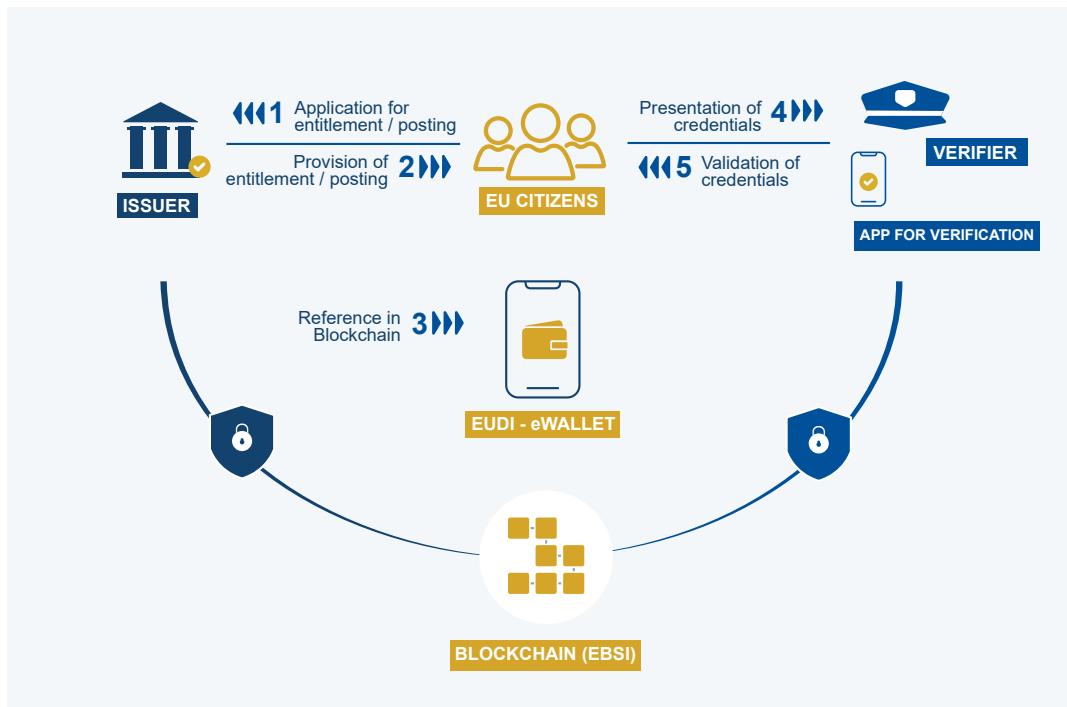


Figure 11: The conceptual architecture for the information exchange and verification processes related to verifiable credentials in DC4EU.¹⁰⁸

In France, France Identité was launched in 2022, was one of the early adopters of the digital identity wallet concept. Initially France Identité was an updated version of the digital identity aimed to comply with the eIDAS regulation, while remaining compliant with the particularities of the French administrative system (e.g., lack of a central population registry, lack of personal identification codes, optionality of the national identity card, etc.).¹⁰⁹ The fact that France Identité functions as an identity wallet allowed to integrate different credentials, the first of which was the driver's license, which can be saved in the application along with the identity card since February 2024.¹¹⁰

EU Digital Identity wallets will serve a wide range of online and off-line usecases, including mobile driving license, accessing onlinen public and private services, opening a bank account, SIM registration, payment authorisation, authenticating a third-party service to sign documents, digital travel credentials, etc. Implementation of these use-cases using the abovementioned EUDI Wallet's reference implementation is currently being tested in four large-scale pilot projects funded by the EU.

¹⁰⁸ Adapted from: DC4EU webpage available at <https://www.dc4eu.eu/project/wp6/>

¹⁰⁹ <https://france-identite.gouv.fr/en-savoir-plus/de-quoi-s-agit-il/>

¹¹⁰ <https://france-identite.gouv.fr/articles/le-permis-de-conduire-integre-France-Identite.html>



The Potential consortium involves 19 EU Member States and Ukraine, bringing together over 140 public and private entities. The project will pilot six use cases.

eGov services: using digital identity to access citizenship procedures online.

Bank account opening: a fully remote procedure for opening a bank account using digital ID.

SIM car registration: using digital ID for activating mobile phone contracts, including cross-border subscriptions.

Mobile driving licence: storing a driver's licence as a digital credential, which can be accepted by car rental agents or police officers throughout Europe.

Qualified e-signature: using digital ID to electronically sign documents, including in the context of cross-border procedures.

e-Prescription: using digital ID to fill/re-fill prescriptions throughout the EU.



The DC4EU consortium involves 20 EU Member States as well as Norway and Ukraine. The project will focus on the use of EUDI Wallet for digital credentials in two domains: education and social security. In the education domain, the project will design and implement activities for educational credentials and professional qualifications. In the social security domain, DC4EU will design and implement activities for entitlement documents (Posted Worker Document A1¹¹¹ and European Health Insurance Card¹¹²), including the implementation of a reference architecture for social security, onboarding customisation and execution for social security institutions, health care providers and public administrations.



The EU Digital Identity Wallet Consortium involves representatives from 27 EU Member States and other countries. The project will pilot the implementation of the EUDI Wallet in focusing on e-commerce in the area of travel services. To support the implementation of the travel use-case, the project will develop two building blocks: cross-border payments solution and organisational digital identity. The main objective is to ensure secure eCommerce for both customers and service providers.



The NOBID consortium involves 6 EU/EEA Member States and focuses on enabling the use of national eID solutions across the Nordic and Baltic regions in the area of payment services (both national and cross-border). The payments use-case is key to the potential development of the Digital Euro, and is based on the existing infrastructure used for bank payments, including SCT instant payments as well as the more traditional account-to-account transfers. The piloted solution will build on the basis of a payment request issued by the recipient, with several interaction modalities, including QR codes, push notifications and deep linking. It will ensure strong customer authentication and transaction linking in compliance with the PSD2¹¹³ requirements.

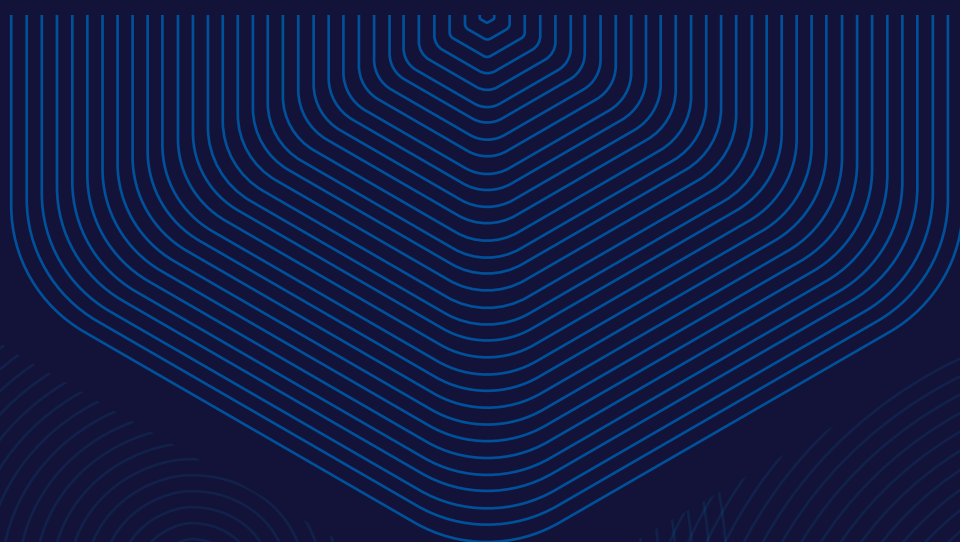
¹¹¹ Posted Worker Document A1

¹¹² European Health Insurance Card

¹¹³ Directive (EU) 2015/2366, OJ L 337, 23.12.2015, p. 35–127

4

DIGITAL IDENTITY ENABLING ACCESS TO HUMANITARIAN SERVICES IN MIGRATION



4. Technologies enabling access to humanitarian services for undocumented individuals

Advancements in technology and digital identification have paved the way for progress in various global domains. One significant area that could benefit from digital ID systems is the field of asylum, particularly in cases involving displaced individuals and in the context of humanitarian crises. The recognition of the identity or a particular status (e.g., refugee), plays a pivotal role in addressing the basic needs and providing support for refugees and asylum seekers. Unfortunately, obtaining and maintaining traditional identity papers throughout the journey of a displaced individual is often a challenging process, leaving them in a state of uncertainty in the receiving country. This can lead to unnecessary delays in accessing essential support services or addressing the primary needs and rights, such as opening a bank account or acquiring a SIM card. To address these challenges, there is a growing exploration of digital ID systems as potential solutions, aiming to streamline processes and enhance the efficiency of support mechanisms for those in need. As stated by the World Bank proof of identity is a “key enabler” for access to services and a trusted digital ID system can strengthen effectiveness and transparency of public services delivery¹¹⁴. Digital ID can also be used at a smaller scale within refugee camps or hot spots, in order to manage the resources available to each individual and transparently track their application journey.

One project is piloted by the UN in a Jordan refugee camp, and another by the Finnish government using a prepaid card systems associated to a digital ID to distribute financial assistance and giving access to the main digital systems in Finland¹¹⁵.

The United Nations has incorporated digital identity into the Sustainable Development Goals (SDGs) 2030 agenda¹¹⁶, underscoring a commitment to the principle of “leaving nobody behind, even in the digital space”. The UN’s overarching strategy considers refugee registration an essential component within a multi-sectoral and versatile ID infrastructure. The UN Refugee Agency (UNHCR) began aiding its member states in the establishment of robust digital refugee registration systems equipped with data security and privacy standards to ensure the protection of the rights and well-being of registered individuals. The UNHCR has been advocating for the development of digital ID specifically for undocumented and underserved groups like refugees and introduced a suite of digital identity tools. In the UN context, the Population Registration and Identity Management Eco-System (PRIMES)¹¹⁷, is a centralized registration platform for identity management tools and applications that prioritize facilitating direct access by individuals of concern, granting them access to personal data, entitlement accounts, and identity wallets. PRIMES¹¹⁸ integrates a number of identity

114 **Inclusive and Trusted Digital ID Can Unlock Opportunities for the World’s Most Vulnerable** ([worldbank.org](https://www.worldbank.org))

115 **Fraunhofer FIT - Blockchain-based Asylum Process Management** ([uni-bayreuth.de](https://www.uni-bayreuth.de))

116 <https://sdgs.un.org/goals>

117 **Registration tools – UNHCR – Guidance on Registration and Identity Management**

118 More information about each individual tool is available here: <https://www.unhcr.org/registration-guidance/chapter3/registration-tools/>

management applications, including proGres¹¹⁹, the Biometric Identity Management System (BIMS)¹²⁰, the Global Distribution Tool (GDT)¹²¹, the Rapid Application (RApp)¹²², IrisGuard¹²³, and RAIS¹²⁴, alongside those slated for future development. PRIMES applications are designed to be interoperable with IT systems employed by governments and partner organizations such as the World Food Programme (SCOPE) and UNICEF (Primerio).

Displaced individuals heavily depend on digital networks during their journeys, for various needs such as communication with family, or accessing resources. At the moment, these technologies are not necessarily designed with the specific needs of vulnerable and displaced individuals in mind (e.g., documenting individuals and support for the recognition of a status).

“ **Digital identity technologies could serve as a solution to the challenges associated with proving identity for refugees and asylum seekers**

At European level, technology is utilised primarily for reinforcing border checks and controlling borders and migration flows through tools like Eurodac and Eurosur¹²⁵. Beyond the border control and migration tracking functions, digital identity has the potential to support the work of humanitarian organizations. Digital identity could serve as a solution to the challenges associated with proving identity, stemming from the complexities of obtaining and maintaining identity papers or passports for refugees and asylum seekers. This approach could unlock access to recognition, facilitating

the realisation of individuals' rights. Furthermore, it could offer a digital solution for governments and humanitarian organisations, significantly reducing the need for identification and document collection from both recipients and providers of benefits. Digital identity solutions can also help streamline asylum processes.

Upon arriving in Europe, asylum seekers are often required to register multiple times. Digital identity management with identity issuance and validation through a trusted entity, could allow governmental institutions as well as humanitarian organisations to significantly simplify identity verification processes. In the EU, the new Eurodac, which will store biographic,

119 proGres is the main repository in UNHCR for storing individuals' data.

120 <https://www.unhcr.org/fr-fr/en/media/biometric-identity-management-system>

121 The Global Distribution Tool (GDT) is UNHCR's corporate tool for identity management and assistance tracking at the point of assistance distribution.

122 <https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/05/RApp-FactSheet.pdf>

123 IrisGuard is UNHCR's other primary biometric tool, collecting two iris scans and a facial photo from each individual.

124 RAIS is a web-based assistance management platform to ensure effective tracking of assistance, coordination, and enhanced accountability.

125 European Border Surveillance system https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/border-crossing/eurosur_en

biometric and travel document information to become a case management system that will reduce the need of multiple data entries, facilitate exchange between Member States, speed up the asylum process, follow secondary movements, providing useful information to authorities to adjust the resources needed to manage the flows and support the new resettlement scheme.

4.1. The use of blockchain in asylum context

Digital ID holds great potential for supporting efficient provision of services spanning various organisations and, ultimately, European States. The implementation of a dedicated platform that provides individuals with recognized identification, along with real-time updates on pending procedures and applications, could help streamline asylum procedures and enhance the overall quality of life for asylum seekers and refugees. Utilising the data already collected from asylum seekers upon arrival, such as biometrics and other identity data, could, in certain cases, offer a pathway to providing concrete proof of identity. This, in turn, could facilitate access to the rights and duties associated with recognition in the receiving state.

Blockchain has been long discussed as a technology with significant potential in the area of identity management¹²⁶ (see 3.3.1 above). This approach could ensure a secure, user-controlled, and interoperable foundation for digital identity management in the context of asylum processes.

Below, are presented some use-cases for the implementation of blockchain in the context of asylum procedure.

4.1.1. Blockchain for assistance in asylum procedure – Germany

Germany is pioneering the integration of a federal blockchain infrastructure into its asylum procedures. The Federal Blockchain Infrastructure Asylum (FLORA)¹²⁷ is a blockchain-based support system designed to enhance cross-authority cooperation within the German asylum procedure. FLORA's objective is to minimize the risk of procedural errors, fortify data protection measures, and provide robust safeguards against manipulation. It is one of the flagship projects piloting the application of blockchain technology in public administration in Germany. Currently the project is being rolled out to include sites in Saxon and Brandenburg State. However, the plan extends beyond regional borders, aiming to implement the blockchain system across the entirety of Germany.

The German Blockchain project allows both asylum seekers and authorities to read and write

¹²⁶ See e.g. Yang et.al. 2020. Blockchain-based identity management systems: A review. Available: <https://doi.org/10.1016/j.jnca.2020.102731>

¹²⁷ BAMF - Bundesamt für Migration und Flüchtlinge - The federal asylum blockchain infrastructure (FLORA)

status messages on individual asylum procedures. It does not substitute traditional identification methods but is used to streamline the asylum process. This system fosters more timely and seamless cooperation among the various federal and State authorities involved in the German asylum procedures. The system generates and links “keys” stored in the blockchain as resource locators, that allow State authorities to locate data associated with a particular procedure, which can then be loaded directly from the source system¹²⁸.

One of the main considerations in developing this system is data protection, in compliance with the GDPR. This includes the possibility of rectification and erasure of personal data. A rectification procedure and dedicated privacy service were implemented to allow individuals to request the deletion of their data, for example after the conclusion of an asylum procedure. Both the request and the subsequent deletion are recorded as transactions in the blockchain. A deletion message replaces the information previously linked to the blockchain ID of that asylum procedure.

Further plans explore the potential use of the European Blockchain Services Infrastructure for the Dublin procedure. A dedicated group is working on the conceptualization of this use-case with the Federal Office for Migration and Refugees (BAMF) and the French government. The complexities of integrating a European blockchain system in the asylum context are significant and multifaceted. Challenges arise from the procedural variations and implementation disparities among Member States, compounded by privacy concerns and classification challenges.

4.1.2. Blockchain for access to banking and financial inclusion

In 2015, the Finnish Immigration Service in collaboration with the start-up MONI implemented a prepaid card linked with a digital ID stored on a blockchain¹²⁹. This system allows refugees to access services usually reserved for bank account holders. They could receive State allowance and pay any normal transaction (online and in person) as well as receive wages, allowing asylum seekers to integrate faster and access the job market. Each transaction is documented through the blockchain in a public incorruptible database maintained by a decentralised network of computers that can easily be monitored by the Immigration Service. Since 2019, the Finnish Immigration Service transferred control of the payment cards for asylum seekers to another card provider, PFS Card Services, based in Ireland, following a public tendering process.¹³⁰

¹²⁸ [blockchain-whitepaper-Chancen-Herausforderungen.pdf \(bamf.de\)](#)

¹²⁹ [How Blockchain Is Kickstarting the Financial Lives of Refugees | MIT Technology Review](#)

¹³⁰ [Moni payment cards used by asylum seekers to be replaced by PFS cards in April 2019 – Moni cards will stop working on 30 April | Maahanmuuttovirasto \(migri.fi\)](#)

4.1.3. Blockchain for the streamlining of humanitarian aid towards ID recognition

In 2017 the UN's World Food Program (UNWFP) launched a blockchain integrated biometric authentication system to the Syrian refugee camp of Azraq in Jordan¹³¹. The UNWFP distributes cash-for-food aid to refugees who can pay at the supermarket not through a card but using a biometric scan of their retina. Transactions are recorded on a private Ethereum-based blockchain, called Building Blocks. This system has allowed the UN to transfer cash instead of delivering food, bypassing the limitations and fees of local banks. Building Blocks was born out of the need to save money, which was being spent through the delivery system. However, traditional banking would not have been a viable solution as generally banking is not possible for individual without approved ID which often refugees could not provide easily, on top of the transaction fee cost which would have been a large additional cost. Furthermore, this solution allows refugees to access more than food, but provides a pathway to recognised identification. The transactions recorded on the blockchain could be used as a credit score history to be recognised beyond the borders of the UNHCR's refugee camp. The use of Building Blocks has expanded and is being used in Bangladesh, Lebanon, and most recently Ukraine. In Bangladesh, the tool supported the distribution of e-vouchers to refugees in the world's largest refugee camp in Cox's Bazar. In Lebanon and Ukraine, the tool helped different humanitarian organisations coordinate and streamline their operations, ensuring that there is no overlap in terms of support provided by different aid organisations, and that support reaches the right people at the right time and as efficiently as possible.¹³²



Figure 12: UN WFP, Building Blocks: How does it work¹³³

131 Inside the Jordan refugee camp that runs on blockchain | MIT Technology Review

132 <https://innovation.wfp.org/project/building-blocks>

133 ibid

Conclusion

This report provided an overview of the developments in identity management technologies in the context of international travel and migration. From the literature surveyed in the preparation of this report, it is safe to say that identity management in the context of international travel emerged largely in the past century, and in this relatively short period of time in historical terms, has undergone a very significant evolution. This evolution has been driven largely by the development of computing technologies, which evolved in parallel, and enabled the continuous digitalisation of identity management processes.

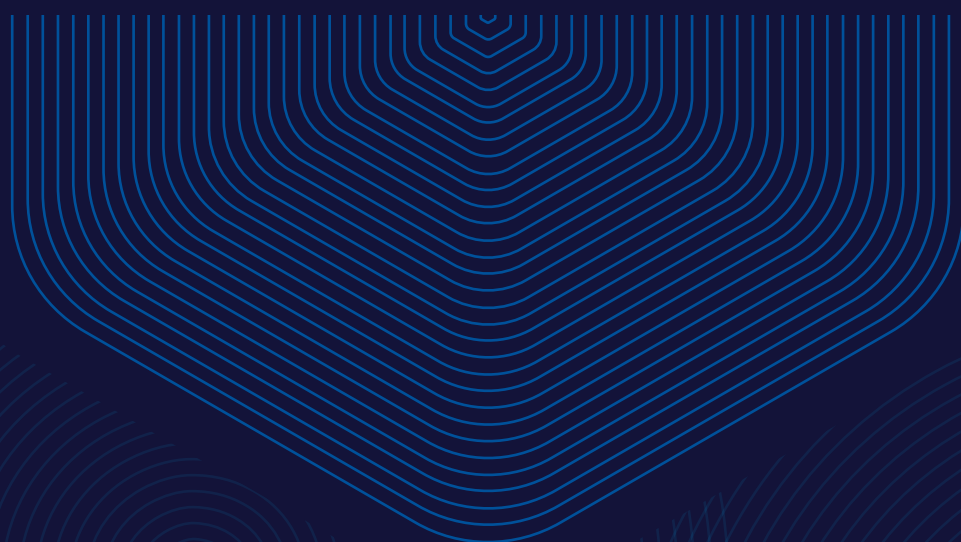
Even though today we still rely on physical identity documents for identity verification purposes when travelling, most identity management processes that support international travel take place in the digital realm. In fact, a passport today is simply a physical representation of data stored in a civil registry or a similar digital system, and a significant share of travel documents issued around the world today include a chip that carries a digital copy of biographical data, as well as biometric data.

These developments in identity management technologies have supported the steady increase in international travel, while further enhancing border security and the security of international travel itself. In fact, the developments of identity management technologies, in particular in biometric recognition and digitalisation of identity, have provided solutions to balance the demands for more open, and at the same time, more secure borders. The continued evolution of identity management will be driven by technological innovation and regulatory advancements. The implementation of the EU Digital Identity Wallet and the proposed EU Digital Travel application are indicative of the shift towards more integrated and user-centric identity solutions. As these technologies mature, they will likely lead to more seamless cross-border travel experiences and improved access to services for undocumented individuals.










Of course, innovation in identity management, as in other areas, does not come without its own challenges and risks. As digitalisation continues to expand, identity management systems must adapt to meet the challenges of privacy, security, and accessibility, ensuring that they support both governmental functions and individual rights in an increasingly interconnected world. Digitalisation also opens opportunities for identity fraud at larger scale than was ever possible before, whether relating to the use of Generative AI for impostor attacks in biometric systems, or identity theft and misuse on the internet. It is therefore essential to continue investing in research and technology development that will ensure the secure and safe use of identity management technologies in the future. Moreover, it is even more important to incorporate these more advanced and secure technologies in the systems operated by public sector authorities such as eu-LISA.

5

ANNEXES



Overview of the systems managed by eu-LISA

Asylum, migration and borders		
	<p>Eurodac is the EU database of digitalised fingerprints for managing asylum applications under the Dublin Regulation. The system assists in establishing the responsible Member State by determining whether the applicant has previously claimed asylum in another EU country. To better combat irregular migration, eu-LISA will undertake a major evolution of the system, introducing new functionalities and central system redesign.</p>	 In operation
EU internal security and borders		
	<p>SIS is the largest information-sharing system for managing external borders and ensuring the internal security of the Schengen area. SIS facilitates information exchange about wanted or missing persons or objects, together with instructions for competent authorities on what to do when the person or object has been found. As such, it serves as an invaluable tool for combatting cross-border crime and terrorism.</p>	 In operation
Schengen, borders and visa		
	<p>VIS facilitates the processing of visa applications and the management of short-stay visas for TCNs travelling to or transiting through the Schengen area. It supports the implementation of the EU's common visa policy and helps combat visa fraud by assisting in the identification of persons not fulfilling the necessary conditions for stay or entry.</p>	 In operation
	<p>EES is set to streamline border control procedures by replacing manual passport stamping with the electronic registration of all third-country nationals entering and exiting the Schengen area. Once operational, EES will ensure better monitoring of authorised stays and the identification of possible overstayers, thereby contributing to preventing irregular migration and strengthening internal security, while also helping to combat organised crime and terrorism.</p>	 In Development
	<p>ETIAS is an online travel authorisation system for visa-exempt third-country nationals travelling to 30 European countries. This pre-travel screening system will compare information across all JHA systems, as well as Europol and Interpol databases, for advance identification of potential security, irregular migration or high epidemic risks that may give grounds for denying entry to the Schengen area. ETIAS travel authorisations are checked by air, sea and land carriers prior to boarding and also by border guards at Schengen borders.</p>	 In Development

Justice cooperation



ECRIS is a decentralised system for exchanging information between Member States on criminal records of EU citizens. ECRIS RI offers an integration interface which enables connection between national criminal record registers of Member States.



In operation



ECRIS-TCN will facilitate the electronic exchange of information on the criminal records of third-country nationals and stateless persons. As such, it supports the principle of mutual recognition of sentences and judicial decisions across Europe.



In Development



e-CODEX is a communication platform for facilitating the secure transmission of electronic content between judicial authorities and legal professionals in cross-border proceedings, ensuring a more efficient judicial process for citizens and businesses across Europe. eu-LISA will be responsible for the e-CODEX system starting from 3 June 2024.



In operation



The Joint Investigation Teams collaboration platform will facilitate communication and cooperation between European judicial and law enforcement authorities, relevant EU agencies, and the European Anti-Fraud Office (OLAF), with a view to improving the efficiency and effectiveness of cross-border investigations and prosecutions.



In Development

Interoperability



Interoperability is the capability of interconnected systems to share data and exchange information, providing relevant authorities with streamlined access to comprehensive information.

The overarching systems interoperability for the JHA domain will be enabled by the following components that facilitate authorised searches and information exchange:

European search portal (ESP) enabling authorised users to conduct single searches and receive results from all JHA information systems they are authorised to access,

common identity repository (CIR) provides a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN,

multiple-identity detector (MID) creates and stores links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud,

shared biometric matching service (sBMS) matching an individual's biometric data across different systems.



In Development



Manuscript completed in April 2025.

This document is public. Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.

Luxembourg: Publications Office of the European Union, 2025

ISBN 978-92-95237-00-1 doi:10.2857/2156066 Catalogue number: EL-01-25-004-EN-N

© European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) 2025