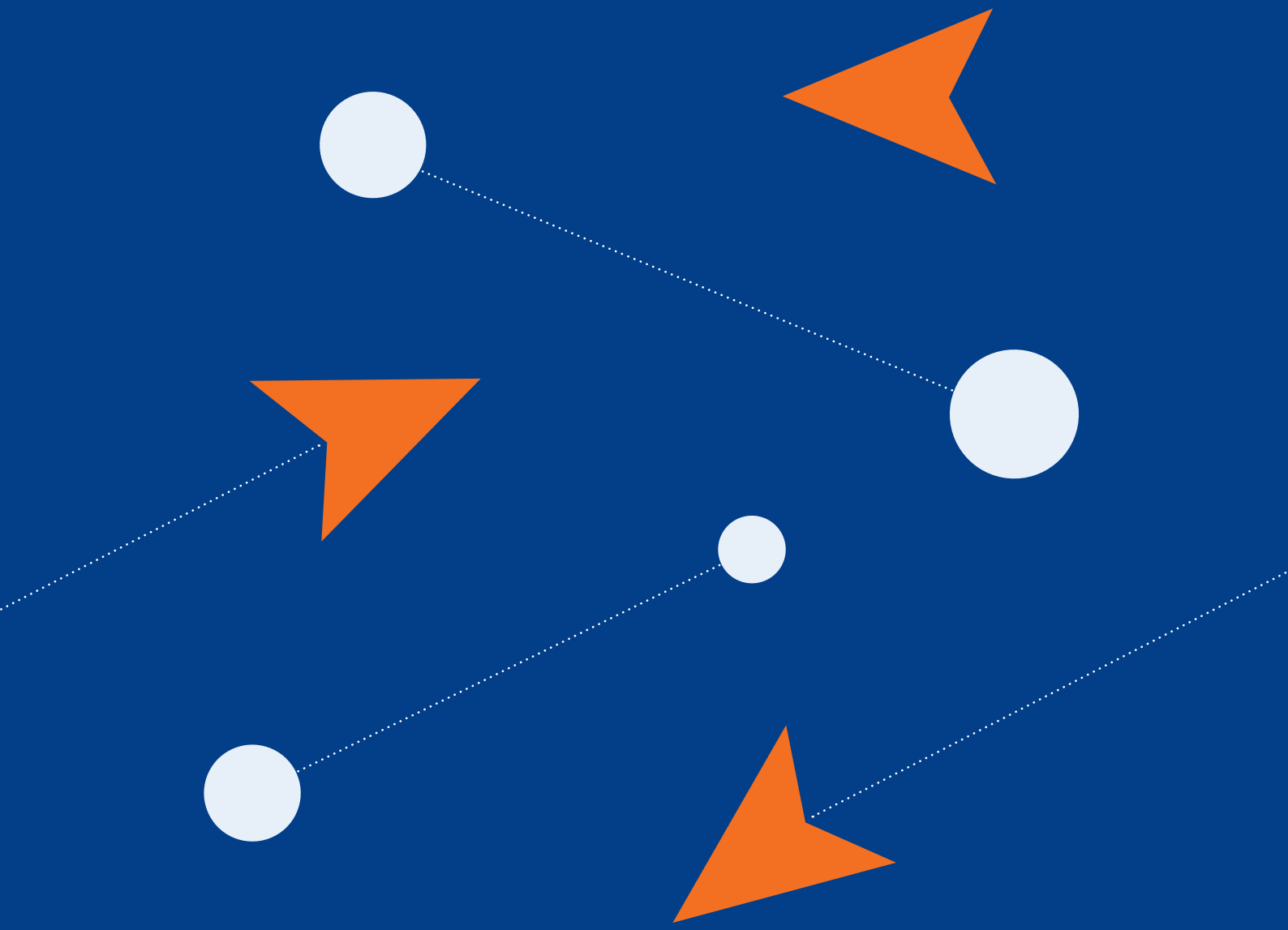


IOM DIGITAL IDENTITY TOOLKIT

COMPASS
Guiding safe migration

IOM
UN MIGRATION

Ministry of Foreign Affairs of the Netherlands

IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM acts with its partners in the international community to: assist in meeting the operational challenges of migration; advance understanding of migration issues; encourage social and economic development through migration; and uphold the human dignity and well-being of migrants.

This publication adheres to the IOM Legal Identity Strategy which lays the foundation for supporting individuals, States, and governments to meet Sustainable Development Goals (SDG) Target 16.9 and Objective 4 of the Global Migration Compact for Migration.

This publication was made through the support IOM's Cooperation on Migration and Partnerships for Sustainable Solutions (COMPASS) initiative, designed to protect people on the move, combat human trafficking and smuggling and support dignified return and sustainable reintegration. The programme focuses on systemic changes that are critical to addressing the underlying causes of migrants' vulnerability, gender equality and exclusion, including in humanitarian and fragile settings; supporting rights-based policies and legislation; equitable access to essential protection services; strengthening local partnerships for migrant inclusion and social cohesion; access to legal identity; reinforcing data-driven responses; and influencing social behaviours and norms. The programme is being implemented in partnership with 14 partner States.

Publisher: International Organization for Migration
17 Route des Morillons
P.O. Box 17
1211 Geneva 19
Switzerland
Tel.: +41 22 717 9111
Fax: +41 22 798 6150
Email: hq@iom.int
Website: www.iom.int

This publication was issued without formal editing by IOM.

Required citation: International Organization for Migration (IOM) (2025). *IOM Digital Identity Toolkit. Immigration and Border Governance Unit.* IOM.

Coordination: Nelson Goncalves, Aijan Boronbaeva, Julia de Bresser, Isabella Dourado

Design: We2Co

ISBN 978-92-9268-996-4 (PDF)

PUB2025/030/R

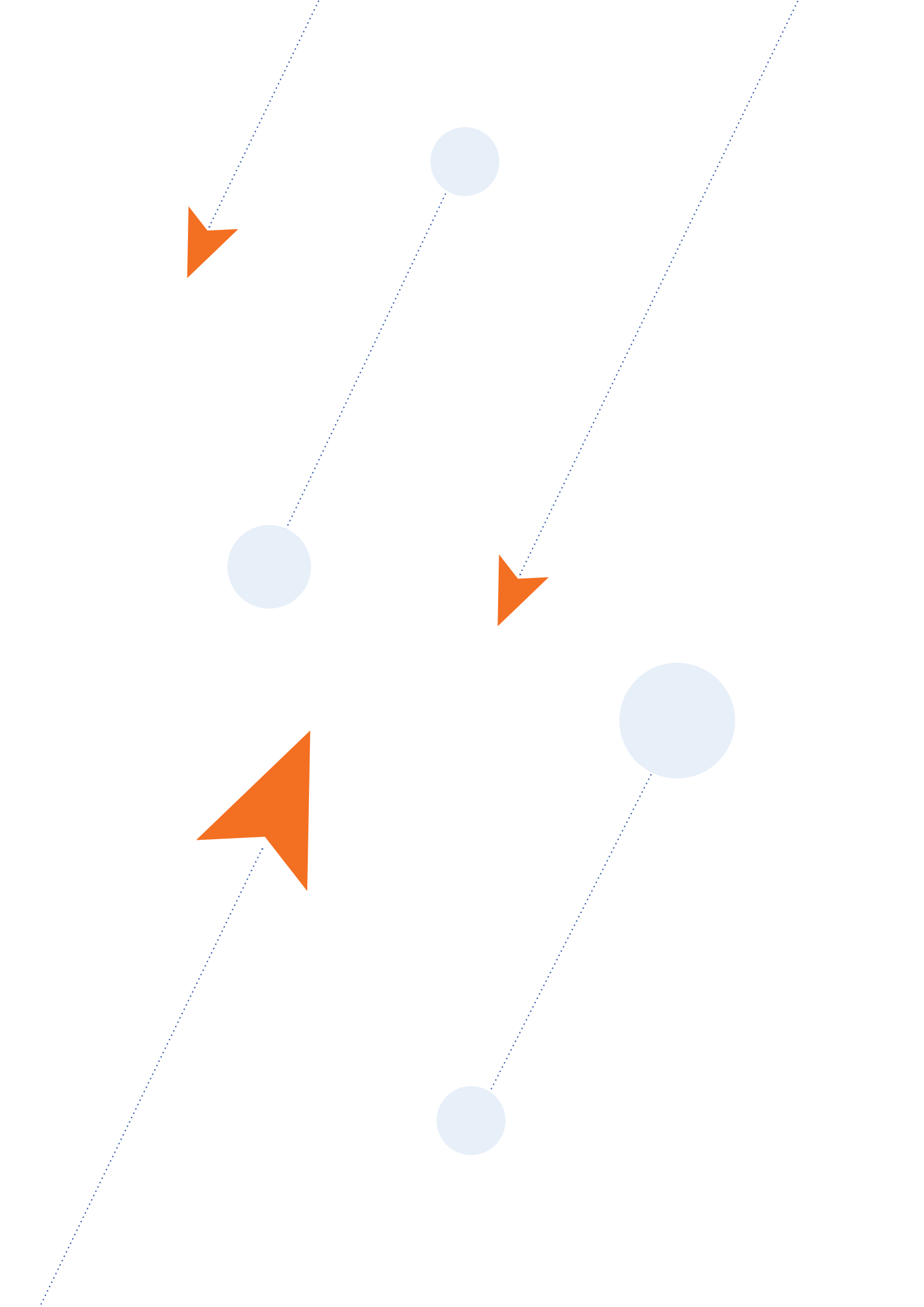
IOM DIGITAL IDENTITY TOOLKIT

Florian Hoefle

COMPASS
Guiding safe migration

IOM
UN MIGRATION

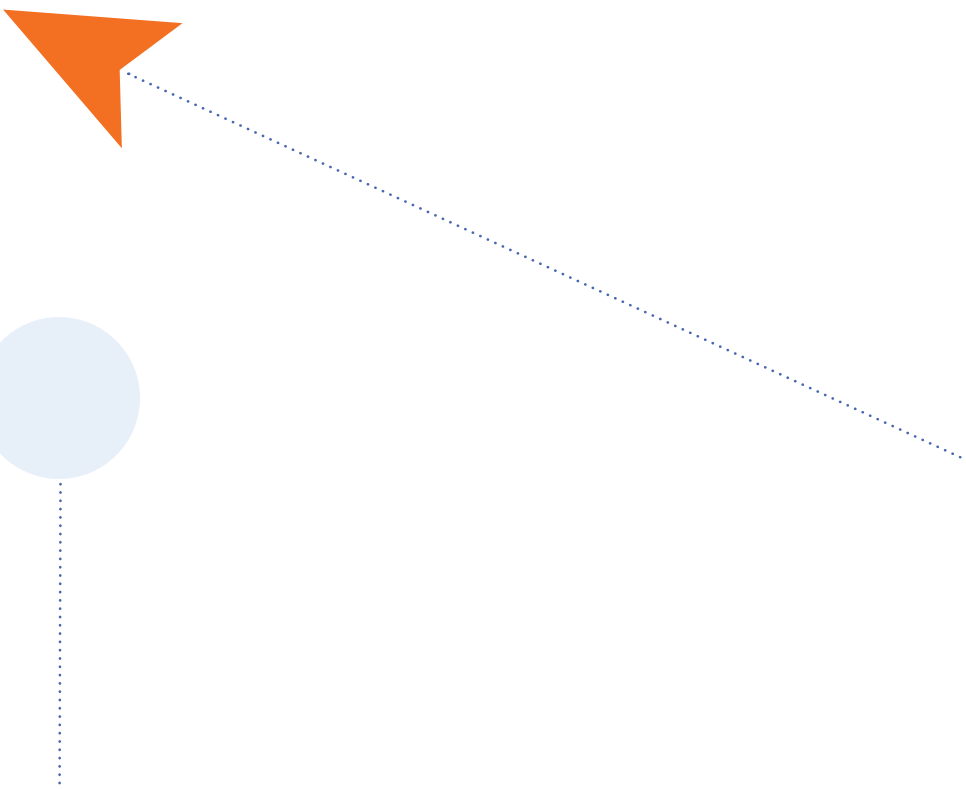
Ministry of Foreign Affairs of the Netherlands



CONTENTS

LIST OF TABLES

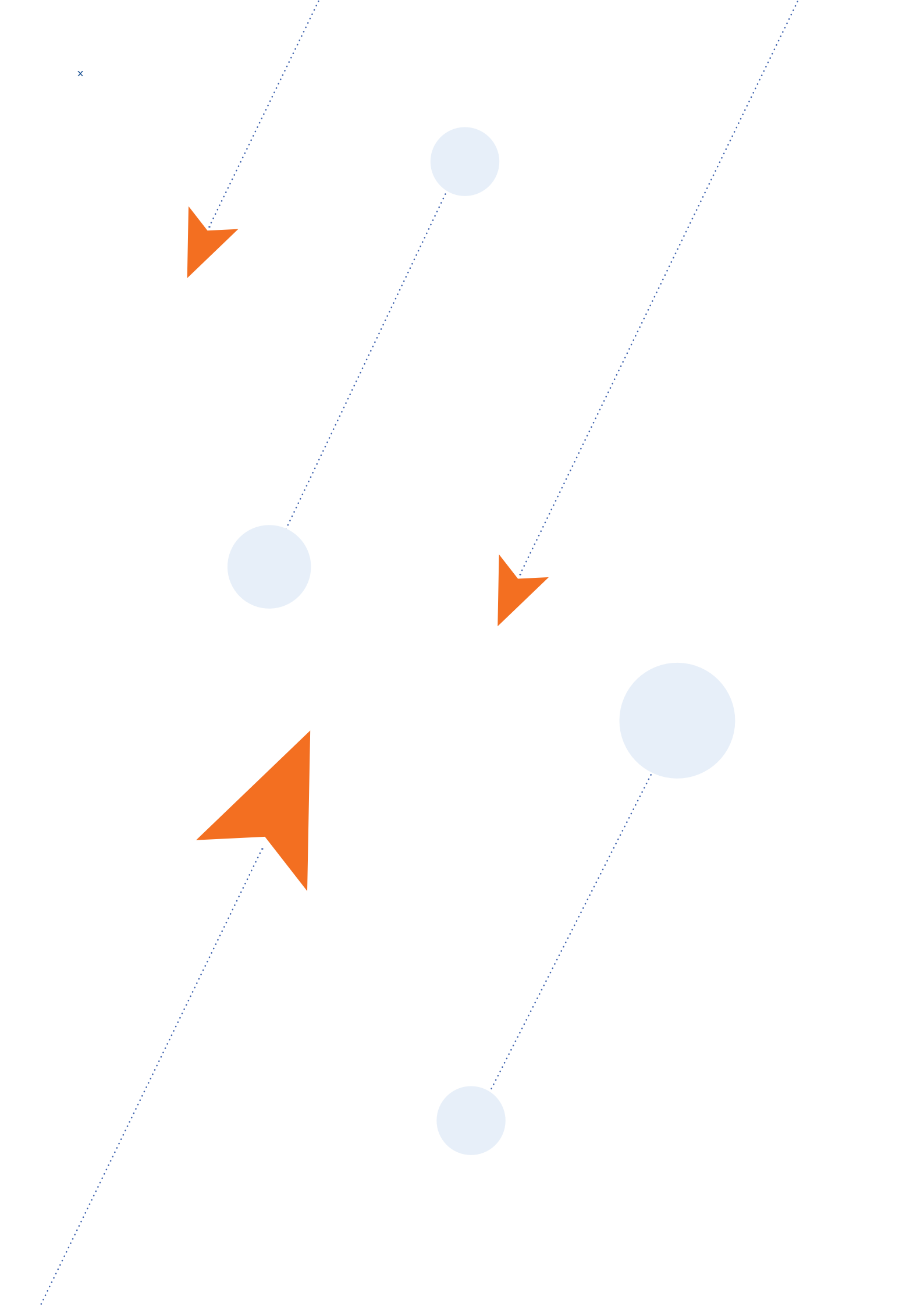
LIST OF FIGURES



ABBREVIATIONS

2FA	Two-factor authentication (requires a user to not only enter a password but also to receive a challenge through different communication channels as a second layer of security)
ABC	Automated Border Control
CA	Certificate Authority (term of the PKI infrastructure and holding a private key)
CSCA	Country Signing Certification Authority (term of ICAO for a Root CA signing Travel documents for a country)
CAPEX	Initial implementation costs
Digital ID	The representation of a digital identity based on a digital identity credential installed on a personal mobile device of the identity owner
Digital Identity System	The term "Digital Identity System" includes the Digital ID application on mobile devices, the related back-end and front-end systems. It covers the entire system infrastructure for the operation of a Digital ID implementation
DIS	Digital Identity Systems
DTC	Digital Travel Credential (a form of Digital ID proposed to complement e-Passports)
eIDAS	Electronic Identification, Authentication, and Trust Services (refers to a range of EU European Union standards for services that include verifying the identity of individuals and businesses and verifying the authenticity of electronic documents)
eSignet	Product name of the open-source Single Sign On solution provided as open source by the MOSIP Project
ETA	Electronic Travel Authorization
FMZ	Free Movement Zone
HSM	Hardware Security Module (a special secure module to store secret keys and digital signature keys)
ICAO	International Civil Aviation Organization
KYC	Know Your Customer describes processes where a provider authenticates a customer to a certain assurance level to perform regulated transactions
mDL	Mobile Drivers License (a term for defining a drivers' license represented as digital credential in a mobile application)
MOSIP	Recognized digital government infrastructure project of the IIIT college of Bangalore, available in open source

NFC	Near-Field Communication (RFID technology used for short-distance data communication)
OPEX	Ongoing operational costs
PKD	Public Key Directory (in the context of the ICAO-PKD, is a system for exchanging public certificates to validate international travel documents)
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification (contactless transmission)
SIM	Subscriber Identification Module (electronic as eSIM or physical card)
SMS	Short Message Service (provided via mobile networks like GSM/3G/4G and LTE)
SSO	Single Sign On (a technology to allow the access to multiple web platforms with a single login credential)
TRIP	Traveller Identification Programme (of ICAO)
TSL	Trust Service Lists or Master list
TSO	Trust Service Authorized Operator
TSP	Trust Service Provider
UID	Unified ID Number
VC	Verifiable Credential (a digital credential which can be verified)
VDS	Visible Digital Seal (a data token which that is digitally signed to ensure integrity and presented in a 2D barcode for easy readability)



INTRODUCTION

The Digital Identity Toolkit aims to enhance stakeholders' understanding of establishing and implementing digital identity, with particular attention to human rights, including privacy, security and essential technological considerations. When implementing a digital identity, safeguarding data privacy, preventing discrimination and supporting equitable access to services are crucial. The widespread growth of smartphones presents an opportunity to expand reach, close gaps in service provision in remote areas and enhance the availability and quality of public services.

This toolkit serves as a practical guide for policymakers and practitioners on operationalizing and implementing digital identity frameworks and systems. It offers strategic insights into cases, guidance on setting up a digital identity programme and a technical background. The document's audience consists of decision-makers and policymakers with knowledge and understanding of government services and general IT and technological knowledge.

Digital Identity

The digitalization of government services plays a crucial role in fostering economic and social development, aiming to include the entire population without leaving anybody behind. An individual's identity within a country is established through legal identity, verified and registered by the responsible authority in the civil registry. Following the registration, proof of legal identity is issued – as a paper or physical card. As electronic government services advance rapidly, the need arises for a secure digital counterpart, or "digital pendant," to the physical identity document. This digital identity enables secure access to and interaction with government services. In many contexts, digital services help expand the reach and availability of government support, providing 24/7 access and lowering the cost-of-service delivery.

Digital identity connects an individual's legal identity to the digital realm, providing secure digital proof like the role of a national identity document (ID) card in the physical world. According to the United Nations Legal Identity Agenda, legal identity is defined as "the basic characteristics of an individual's identity, e.g. name, sex, place and date of birth, conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death.[1])."

By bridging this foundational legal identity into digital systems, digital identity serves as a secure means for individuals to interact with government services, such as education and tax voter registration, offering a mechanism for verifying and protecting identity across digital applications. Within national legal and social ecosystems, digital identity enhances public service accessibility and security, enabling individuals to access services efficiently and securely. Digital identity can also support cross-border identity management, facilitating international cooperation through bilateral or multilateral agreements within economic or political zones. While beneficial, these agreements introduce additional legal and policy complexities alongside technical challenges.

Beyond the large-scale implementation of general Digital ID systems, simplified Digital ID solutions can offer practical benefits for both citizens and governments. For example, migration management and movement between neighbouring countries can be facilitated through bilateral agreements that allow the use of a mutually recognized digital identity within a free movement zone, eliminating the need for an International Civil Aviation Organizatio (ICAO) compliant travel document. This approach reduces investment and operational costs associated with managing movements within the zone.

1 United Nations Legal Identity Agenda.

Digital identity frameworks vary widely and are often highly customized, with features tailored to specific needs and, at times, complex implementations. The technology driving digital identity is often developed by highly industrialized countries and may not always align with the needs of lower-income nations. A prerequisite for a Digital Identity System (DIS) is the existence of population databases and registration systems capable of processing biometric data, providing a foundation for clearly defining individuals' identities. The planning and implementation of a digital identity system can, in turn, support improvements in digital population registers and related biometric systems.

To function effectively, a digital identity system requires integration with other applications, which can introduce additional complexity and costs. When implementing such a project, careful planning is essential to balance costs, benefits and operational requirements.

Digital Identity in Migration Contexts

Identity provision is essential, and even more so for vulnerable populations. Reliable identity systems help to safeguard and protect migrant populations, including refugees, internally displaced persons (IDP) and stateless individuals. For many migrants, the absence of a recognized identity document can mean limited access to health care, education, employment and legal protections, exacerbating risks of exclusion and exploitation.

DIS can contribute to addressing these challenges, though barriers remain. Issues such as limited access to technology, gender disparities and discrimination can restrict access to digital identity solutions, particularly among undocumented migrants and individuals in remote areas. Recognizing these realities, this Digital ID Toolkit encourages approaches that acknowledge and aim to mitigate these barriers, ensuring digital identity systems are accessible and inclusive.

For migrants, the registration process – including the secure capture of biographical and biometric data – lays a foundation for inclusion, much like population registration, while accounting for the unique vulnerabilities and needs of mobile populations. This toolkit supports practical strategies for issuing identity documents with digital credentials in physical and/or digital formats, emphasizing that such processes should prioritize a human rights-based approach, addressing inequalities and safeguarding dignity.

The IOM Digital ID Toolkit

The IOM Digital Identity toolkit guides States in the introduction and implementation of a digital identity through accessible, adaptable strategies. It provides a brief theoretical background on digital identity systems, a credential and general framework, guidance for implementation and practical use case examples.

Limitations

Although the toolkit provides adaptable strategies and an overview of the digital identity management framework, the solutions may not fully address the unique legal, social and other requirements, including financial investments into digital technologies, of each Member State. Local contexts may require further customization, which could lead to complexity and added costs. In addition, the toolkit aims to support large-scale implementation, but scalability could be a challenge in countries with limited infrastructure or large populations lacking digital access. Therefore, the physical components, including issuing cards or tokens, may face logistical and distribution obstacles. The toolkit and its solutions provide an overview of digital identity management and demonstrate how digital identity functions, specifically in the context of border and identity management, with a focus on pure demonstration purposes. If there is interest in scaling the technical solution, it should be mutually agreed upon with IOM.

The toolkit provides theoretical and practical approaches to digital identity, while stressing the importance of implementing robust data privacy and security measures. For countries with weaker data protection laws or limited cybersecurity resources, ensuring data safety may be difficult, posing a risk of identity theft, misuse or privacy violations. Furthermore, it is worth noting that the toolkit may not fully account for the complexities of integrating new digital identity systems with existing government systems and databases. Therefore, the implementors should consider the importance of smooth integration of the digital identity solution. Overall, the toolkit offers a valuable starting point but may need to be adapted, resourced and supported extensively to overcome these limitations for widespread and effective use.

Part 1: Digital Identity Overview

This section introduces digital identity fundamentals, technologies and best practices for government implementation. It outlines how digital identity management should be structured, including key services and use cases. Over the last decade, many countries have adopted Digital Identity Frameworks, offering insights into effective approaches and challenges. Successful projects are examined to identify critical factors for policy and technology implementation, as well as best-use cases that highlight how digital ID can support government services and enhance access to e-government services. This part concludes with a description of these key technologies and use cases, drawn from lessons learned in existing implementations.

Basics of digital identity and the best practices from several case studies

- Understanding of Digital Identity
- Use-cases of Digital Identity and Key Benefits
- Challenges for Digital Identity Solutions
- Key concepts and technology
- Digital Identity Management Framework
- Best Practices for Digital Identity Management

Part 2: Digital Identity Implementation Guidance

This section offers guidance on implementing a DIS, including operational considerations and potential challenges. Success depends on a country's policy environment and digital infrastructure maturity. The guidance provided is general and adaptable, offering insights applicable to various national contexts. Key prerequisites include a secure digital identity management system and a reliable population register, ideally with biometric data, to ensure unique and verifiable identity links. Biometrics such as photographs, fingerprints or iris scans add a security layer, particularly for mobile-based identity verification. This section also outlines essential implementation steps, including scoping, road map development, key applications and investment planning. To assess readiness, the IOM Digital Maturity Toolkit provides a comprehensive digital maturity assessment, producing a report on the national ecosystem's readiness for digital identity.

Underastanding digital identity management and general steps to follow for implementation

- Governance and General Guidance
- Technical Considerations for Digital Identity Management
- Digital Identity Use Case
- None-& Compliance considerations
- Compliance risks

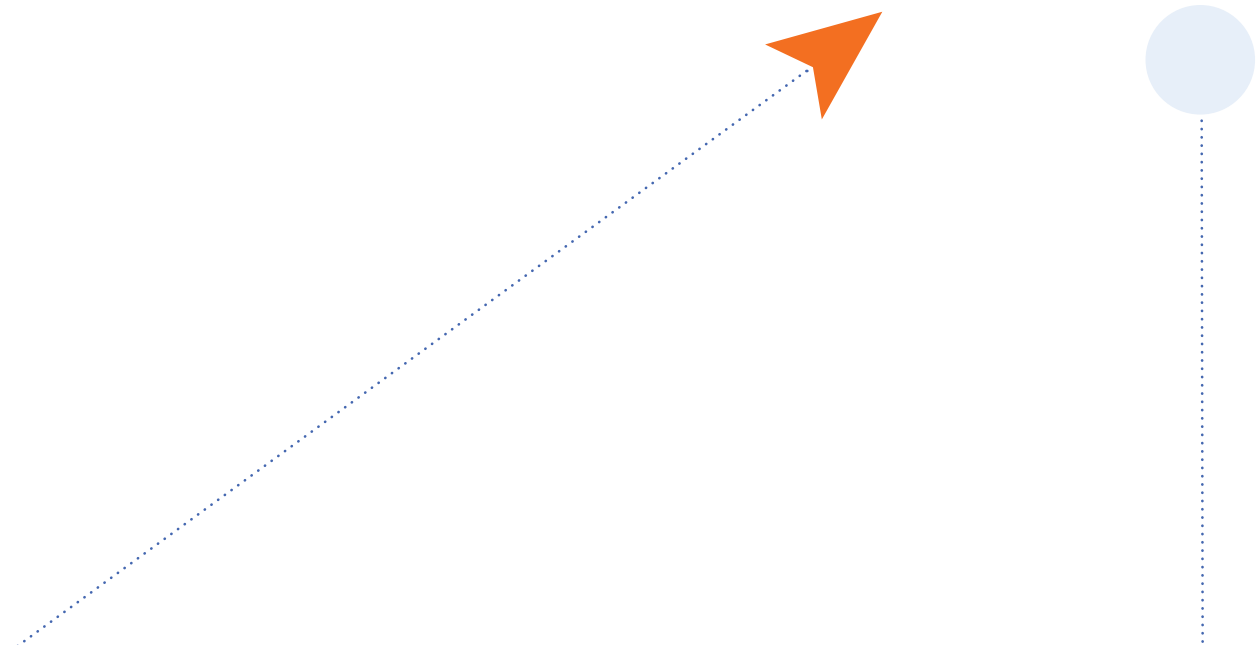
Part 3: Use Case for Digital Identity

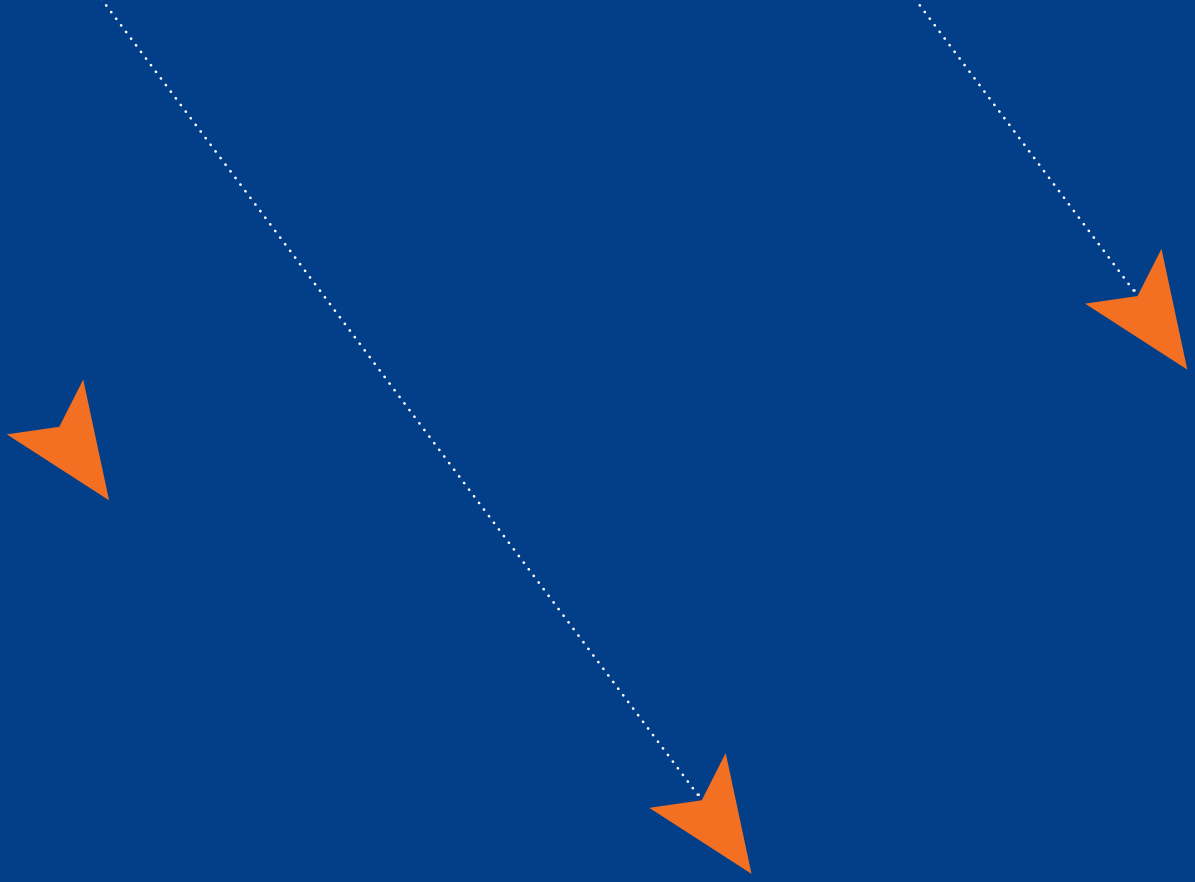
The third part of the Digital ID toolkit describes a migration related use case in which digital identity can be used for border crossing at checkpoints within a defined free movement zone between countries based on a bilateral agreement, where crossings might occur for trade, family, or education purposes. In the case of free movement zones, individuals may not hold ICAO-compliant travel documents.

At border checkpoints when crossing between countries, registration can occur by using a digital identity, physical identity card or paper document, which complement each other using the same verifiable identity credential in the form of a QR code. The different types of "tokens" (paper, ID-card and digital) offer various security and assurance levels for identity verification in both offline and online settings.

Describes a use-case for a digital identity in migration and border management

- Introduction to the use-case
- Key considerations
- Application of the digital identity technologies (mock system)
- System performance
- Mock-up Example





PART 1

Digital Identity Overview

Part 1: Digital Identity Overview

1.1 IDENTITY MANAGEMENT AND DIGITAL IDENTITY CONTEXT

The chapter describes the context of identity management as a prerequisite of a Digital ID.

- Civil registry and legal identity
- Population register
- Biometric and identity attributes
- Unique identity number
- Digital ID prerequisites

1.2 IDENTITY CREDENTIALS

The chapter provides an overview of the Identity credential ecosystem and the relation of Digital ID as part of it.

- Legal identity and national ID
- Digital credentials
- Credential issuing
- Travel identity
- Challenges

1.3 UNDERSTANDING OF DIGITAL IDENTITY

The chapter provides a general overview of Digital ID.

- Digital identity system and Digital ID
- Role of smartphones
- Threats for Digital ID
- Digital ID functionality
- Digital ID ecosystem

1.4 USE-CASES OF DIGITAL IDENTITY

The chapter introduces different use case categories and their requirements.

- Use case – functionality matrix
- Governmental use case
- Regulated private sector use cases
- Private sector use cases
- Special Digital ID use cases

1.5 DIGITAL IDENTITY MANAGEMENT FRAMEWORK

Describes the Digital Identity framework.

- Actors in the framework
- Threats to Digital ID
- Cross border usage
- Trust Service Provider model
- Digital ID ecosystem

1.6 DIGITAL IDENTITY KEY CONCEPTS AND TECHNOLOGY

Technology background and concepts.

- Wallet and Digital ID passes
- Federation concepts
- 2 Factor Authentication (2FA)
- PKI Trust Model
- Visible Digital Seals (technology and potential)

1.7 CHALLENGES FOR DIGITAL IDENTITY SOLUTIONS

The chapter highlights the challenges of Digital ID systems.

- Governance of the Digital ID
- Legal framework and legislation
- Digital maturity
- General digital infrastructure
- Scalability of Digital ID systems
- Use-case planning and key applications

1.8 BEST PRACTICES FOR DIGITAL IDENTITY MANAGEMENT

Examples of generic Digital ID implementation in other countries.

- Digital ID system in Brazil

1.1 IDENTITY MANAGEMENT AND DIGITAL ID CONTEXT

This chapter describes the context of Identity Management Systems, legal identity and relation to Digital ID, emphasizing the essential role of comprehensive identity management in developing secure, unique digital identification systems. Providing accurate and verifiable individual identities in digital formats is a fundamental prerequisite for effective Digital ID implementation.

Legal identity ecosystem

Birth registration constitutes the foundational process for establishing an individual's legal identity within a civil registry system. Upon registration of a birth event under a country's legal framework, an individual acquires a formal legal identity defined by critical demographic data, including the date, time, gender and birth location. Each country's local legislation determines the specific data elements captured during registration. During this process, individuals receive a unique name identifier, which varies across jurisdictions and is expressed according to local linguistic conventions and legal standards.

The birth certificate is the primary and most universally recognized credential of legal identity. It serves as the root documentation of an individual's legal existence and provides a comprehensive record of the fundamental details that establish a person's initial legal standing within a societal framework.

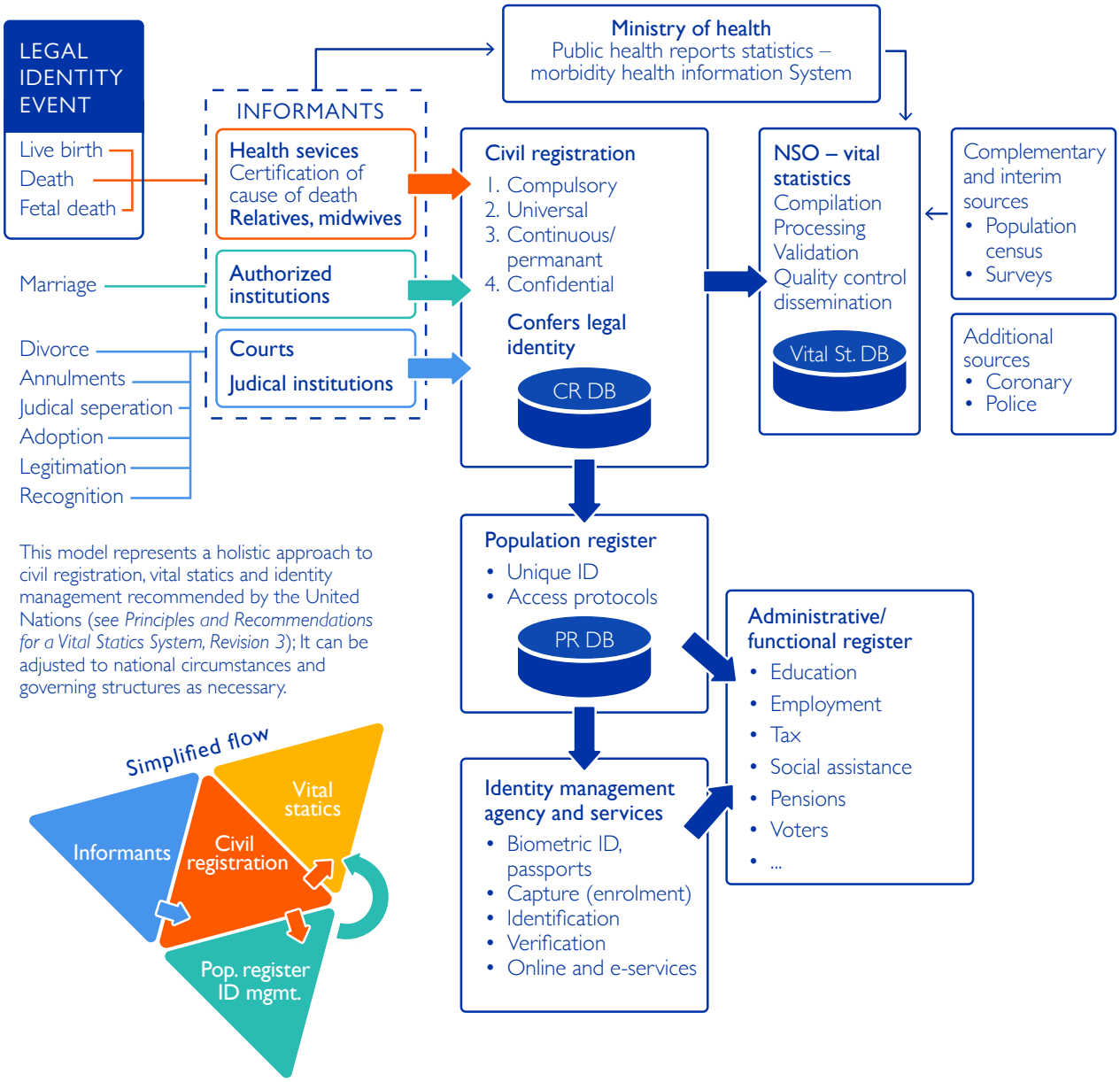
The United Nations[2] emphasizes the importance of a comprehensive civil registration system to document and manage critical life events. In this system, two primary events are pivotal: birth registration, which marks the creation of legal identity, and death registration, which signifies its termination. Additionally, secondary events such as marriages, divorces, adoptions and other significant family-related events are recorded, reflecting the ongoing documentation of an individual's legal status.

In practical digital identity frameworks, such as the IOM Digital ID Toolkit, the population register serves as the primary identity management mechanism. This approach establishes that only individuals with eligible records in the population register can participate in the Digital ID scheme. The methodology recognizes the inherent complexity of identity management systems and the need for tailored approaches that respect each jurisdiction's unique administrative and legal landscape.

The implementation of such systems requires careful assessment of local contexts, understanding that while there are universal principles of identity management, the specific execution must be sensitive to regional variations, legal frameworks, and administrative capabilities. This nuanced approach ensures that digital identity systems are not only technologically advanced but also culturally and legally appropriate for the specific context in which they are deployed.

2 United Nations, *Principles and Recommendations for a Vital Statistics System* (New York, United Nations, 2014).

Figure 1. United Nations holistic approach to civil registration and identity management



1.1.1 POPULATION REGISTER

Legal identities are maintained within a civil registry system, often interconnected with a population register. The structure functionality, and data contained within a population register, as well as its relationship to the civil registry, vary significantly between countries and are shaped by historical development and system evolution.

Typically, a civil registry encompasses all citizens of a country and records vital life events. In contrast, a population register extends its coverage to include legal residents who are citizens of other countries but reside lawfully within the jurisdiction. While the civil registry primarily focuses on individual events, the population register manages identities with additional attributes specific to individuals.

In many cases, civil registries and population registers are integrated within a single database. Whether managed together or separately, each record in the civil registry must be uniquely and securely linked to the corresponding record in the population register. Doing so ensures the integrity and reliability of identity management across both systems.

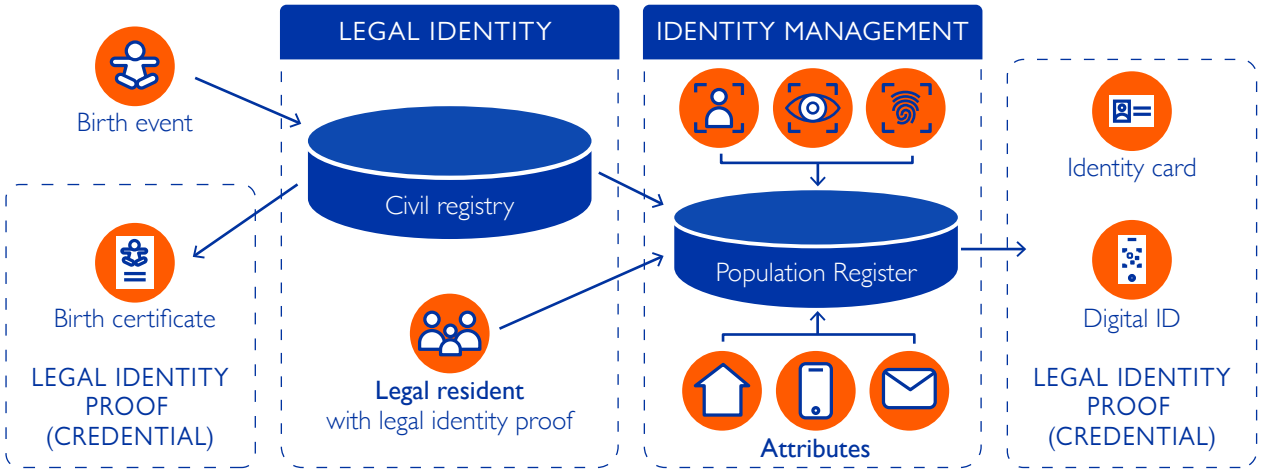
Unique Identity Number

Ensuring the uniqueness of individual records is crucial in identity management, with the most common approach being the assignment of a Unique Identity Number. While some countries prefer using a combination of given name, family name and birthdate as identifiers, this method lacks guaranteed uniqueness and creates challenges in system management.

For population registers without a unique identification number, an upgrade is recommended before implementing a Digital ID. During this upgrade, it is advisable to assess existing unique numbering schemas in other national services like tax or social security. Linking existing unique identifiers to the population register is typically the most efficient and straightforward method, as introducing additional new unique identifiers can potentially confuse citizens and lead to errors in number usage.

The unique identifier can be composed of numbers or a combination of numbers and characters. It is commonly referred to by various terms, including Unique Identity Number, Unified ID (UID) or Personal Identification Number (PIN), with the critical requirement being its absolute uniqueness for each individual.

Figure 2. Identity Management Systems Illustration



Information management process

Managing individual identities and linking them with biometric information is a critical function of the population register. Every piece of information captured, added or modified must be recorded in the database with a secure audit trail providing comprehensive evidence. This evidence can include supporting documents and metadata generated during information changes, with all transactions requiring a digital audit trail that is protected against manipulation.

The audit trail is essential for maintaining a chain of proof, supporting identity-related clarifications and potentially investigating fraud attempts. The accuracy of identity information, biometrics and related attributes is crucial for effective identity management and Digital ID implementation.

Information capture, verification and modification must adhere to strict security policies. It is recommended that information be collected in the presence of both the individual and a government officer. In cases where private companies assist in information capture, a government official must verify and endorse the information before updating population database records.

To protect citizen data and privacy, direct access to population data should be limited to government officials and must comply with local data protection laws. The system should not initiate biometric verifications or demographic data searches without proper legal procedures involving legislative bodies and local courts, in accordance with the country's legal framework.

1.1.2 BIOMETRIC INFORMATION

Biometric information is crucial for individual identification, enabling recognition and verification of identity. When combined with a legal identity credential, biometrics allows a verifier to confirm that the credential's presenter is the rightful person. The verification process can use various types of biometric information and can be conducted either manually by an inspecting individual or automatically through systems and mobile devices, such as when presenting a Digital ID.

Deduplication

Biometric information plays a critical role in deduplication and ensuring identity uniqueness within a public register. A biometric system guarantees that each individual has only one identity that is managed with a link to the civil registry and legal identity.

During the enrolment process, an individual's biometric information is captured and processed. The biometric system cross-checks new enrolments against existing database records to verify that the person has not previously enrolled under another identity. Once the biometric information's uniqueness is confirmed, the individual's population register record is updated. If a biometric match is found, the record is investigated without performing an update.

Identity uniqueness is crucial for all subsequent identity uses, particularly in Digital ID implementation. A unique identity number makes subsequent processes robust and reliable. While alternative methods of establishing uniqueness exist, such as linking names, birthdates and birthplace, these are less reliable and prone to misunderstandings or identity mixing.

An identity number is typically the most secure and common practice. It additionally facilitates identity usage beyond government spaces, enabling linking to physical or digital identity documents without necessarily connecting government and private sector systems.

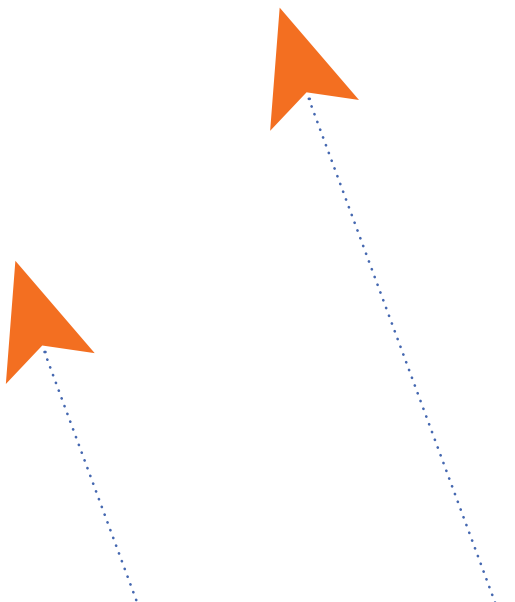
Biometry for identity

The most common biometric identifiers are photographs for face recognition, fingerprints and iris scans. Each biometric type offers unique advantages and limitations for different use cases. Biometric verification involves comparing characteristics using a threshold, with results expressed as the likelihood that two biometric samples belong to the same person.

Face recognition offers ease of use through contactless, distance-based verification and is already incorporated in many existing documents like passports and ID cards. However, it has significant limitations: it cannot distinguish between twins and is vulnerable to morphing – a technique using specialized algorithms to blend two photos into a single image that can potentially allow two different individuals to claim the same identity. To mitigate this risk, it is recommended that photographs be captured live in the presence of a government official.

Fingerprints provide high precision, especially with 10-print capture, but require special verification devices, physical contact and a more costly infrastructure. Despite these challenges, fingerprints offer superior accuracy for enrollment processes and deduplication compared to photography alone.

Iris biometry delivers high accuracy and rapid database recognition. While iris scans can be performed at a distance, achieving higher accuracy typically requires specialized infrastructure. Iris scans are frequently used in airport eGates, often combined with face recognition, with both biometrics capable of simultaneous, distant capture.



Multibiometric systems

A multibiometric system combines two or more biometric technologies to evaluate identity uniqueness or verification. By integrating different biometric technologies, the system achieves higher accuracy while leveraging the advantages of multiple biometric methods. The most common approach involves capturing 10-print fingerprints and a photograph, which together enable verification of uniqueness and can distinguish between twins due to their distinct fingerprints.

For identity document verification, photographs are typically preferred because fingerprint verification requires more complex infrastructure. The COVID-19 pandemic further emphasized this preference, as people became reluctant to touch devices previously used by others. Photographs have become the primary biometric verification method for Digital ID, with smartphone cameras enabling easy face recognition and authentication through liveness detection.

Liveness detection is crucial to prevent manipulation during unsupervised authentication processes. To maintain face recognition performance, it is recommended to update photographs for all registered individuals every 5 to 10 years.

Some countries simultaneously scan the iris when capturing a live photograph, which provides an additional layer of accuracy. This approach is particularly advantageous when enrolling large populations, offering enhanced identification precision.

1.1.3 IDENTITY ATTRIBUTES

During enrollment in the population register, additional personal attributes are captured and stored alongside core identity information. The most common attribute is the address, which represents an individual's permanent living location. Historically, addresses were crucial for personal contact, especially when landline telephones were often shared among multiple people.

The specific additional attributes vary by country but may include information like academic degrees or professional names. Unlike core legal identity information such as family name, these attributes can change frequently. For instance, a family name might change through a legal marriage process, which is recorded in the civil registry and reflected in the population register.

Attributes like living address, email and mobile phone number are particularly prone to frequent updates. All changes must be performed securely, with proper verification and documentation. The correctness and validity of these identity attributes are essential for the effective operation of a Digital ID system.

Capturing of attributes

Attributes are ideally captured during the enrollment or data update process in the presence of a government official. When a population register conducts biometric enrollment, the individual's physical presence is mandatory. This requirement is similar to passport applications, where applicants must be present in person.

The process of adding mobile number and email address attributes should be assessed based on the specific circumstances and available resources in the country.

Authentication of attributes for Digital ID

With the widespread adoption of smartphones and mobile data connections, most people now have a personal email address and mobile phone number. The mobile phone has become a key personal device, and these three elements (email, mobile number and phone) are exclusively used by an individual, making them valuable and mandatory attributes for Digital ID implementation.

Mobile phones enable short message service (SMS) reception through local networks, while email and data connections provide digital communication channels. These two technologies offer important security benefits, with data connections accessible via smartphones and computers, and SMS requiring physical possession of a subscriber identification module (SIM) card.

Verifying these attributes before updating an identity record is recommended. Verification typically involves sending individual random codes via both SMS and email. The individual enters these codes into the system, which confirms the communication channels' validity and accuracy. This process ensures there are no typing mistakes and that the individual has direct access to these channels.

Email addresses and mobile phone numbers are integral to the Digital ID security concept, serving as additional or second-level authentication methods to prevent identity theft and misuse.

1.1.4 POPULATION REGISTER AND LEGAL RESIDENTS

Legal residence refers to individuals living regularly in a country different from their country of origin. The local residence law, governed by the immigration authority, regulates legal processes for foreigners residing in the country. Foreigners enter the country with travel documents such as passports, and undergo a residency issuance process according to local laws.

This process involves acknowledging the foreigner's legal identity and transitioning them into a local legal identity. However, a significant challenge remains: legal identities and their proofs are not currently issued under a global legal and administrative framework that would support cross-border usage of legal identity.

Documents for travel purpose

Travel documents, particularly passports, follow standards established by ICAO through the 1944 Chicago Convention.[3] ICAO Document 9303[4] provides comprehensive technical specifications for visual and electronic travel documents, including passports, ID cards and crew member certificates.

These travel documents are based on legal identities from population registers, prioritizing international travel and border control requirements. This includes standardized name formats, typically mandatory in Latin characters. Legal or local names are not necessarily required for storage on document chips and are primarily personalized on the document's data page.

Travel ID cards require bilateral or multilateral agreements for cross-border usage. Many developing countries prioritize basic identification over travel functionality due to cost constraints. Recent trends include optimizing ID cards for domestic use with Digital ID options or implementing Visible Digital Seal (VDS) technology.

VDS technology, which uses digitally signed 2D barcodes like QR codes, can embed citizens' legal identity and enable both physical and digital verification. Countries may integrate this technology into ID card chips for international interoperability or choose more cost-effective solutions that retain legal identity information through affordable smart chips.

The European Union represents a unique case, recognizing travel documents within the Union as identity documents. This approach is based on a synchronized legislative system and cannot be directly applied to most other countries. Such economic and legal zones require more complex assessment for document and identity management.

3 ICAO, Convention on International Civil Aviation - Doc 7300 (ICAO, 1944).

4 ICAO, Doc 9303, Machine Readable Travel Documents (ICAO, 2021).

Legal identity of foreigners

To overcome the challenge of document legalization, the process is usually performed using the "Convention of 5 October 1961 Abolishing the Requirement of Legalization for Foreign Public Documents,"[5] also known as the "Apostille Convention." The convention is recognized by more than 100 countries, though not by all. For countries not covered by the convention, bilateral processes involving diplomatic missions and local foreign affairs authorities are used to legalize documents for cross-border use.

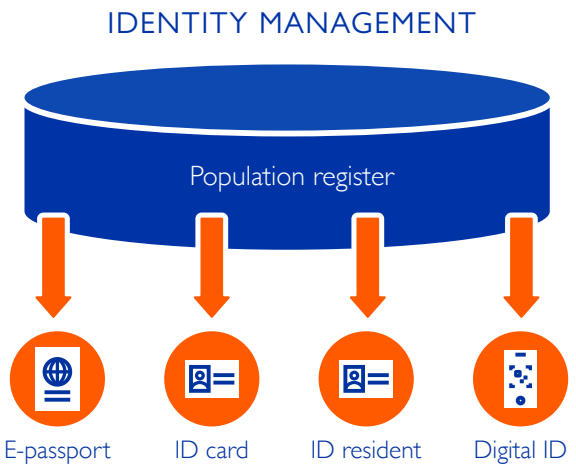
For acknowledging legal identity from one country to another, one of these two processes must be performed. The process results in local legal validity for a document issued in another country. In terms of legal identity, a birth certificate as proof of legal identity must undergo a process of local recognition and creation of a local legal identity, based on the legal identity of a foreigner.

The process involves a certain complexity and discomfort. Some countries practise accepting travel identity as locally valid legal identity, which bears a risk, as in many countries travel identity is highly normalized to Latin characters and sometimes does not include the full name as per the legal identity.

Legal residents participation in Digital ID

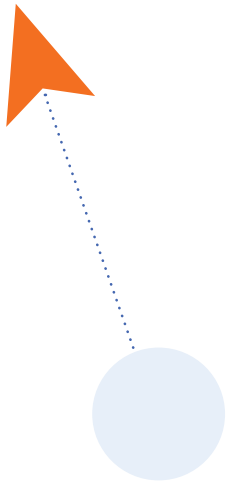
In any case, the process of how a country recognizes the legal identity of a foreigner follows local laws and immigration procedures. If a foreign person is recognized as a legal resident, a document is issued in the form of a residence visa or residence ID card. This document serves as proof of identity per local laws and regulations and is mostly issued from a residence database or population register. Legal residents are part of the population residing in the country and shall therefore be registered in the country's population register.

Figure 3. Document issuance from a population register



In many cases, the enrolment of legal residents in a population register requires a database connection between the immigration systems and population register. For legal residents, the immigration system is the first system to capture their identity, similar to how the civil registry captures the first legal identity for in-country born individuals.

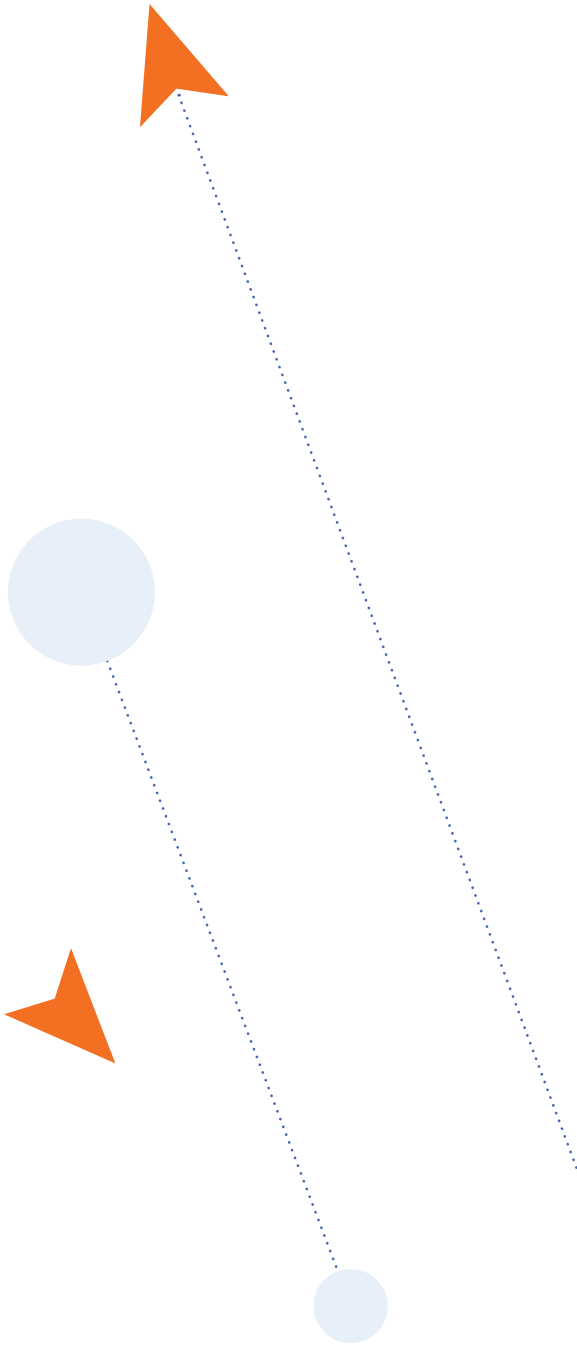
The registration of legal residents in a population register is a prerequisite for participation in a Digital Identity scheme.



5 United Nations, Convention of 5 October 1961 Abolishing the Requirement of Legalization for Foreign Public Documents (The Hague, 1961).

1.1.5 TAKEAWAY AND SUMMARY

A legal identity is created by registering an individual based on a birth certificate and officially acknowledging the identity. A birth certificate is the first proof of legal identity for an individual. A population register links the civil registry for in-country born individuals and immigration systems for legal residents in a central database. Each identity shall have a unique identifier in the form of a unique ID number. It should be used as the primary identifier of everyone in the population register as well as in all other databases to maintain identity data synchronization.



- The population register is a key database for issuing identity documents and Digital ID. The availability of accurate identity information, management procedures and high number of active identity records is a key digital maturity indicator for the implementation of a Digital ID.
- Multibiometric Biometry is key to identify an individual to guarantee the uniqueness of an identity. Most common are face recognition with photographs (for Digital ID and public use cases and database deduplication) and fingerprints for database use.
- The biometric photograph in the public register should be up to date, and it is recommended to renew the photograph every 5 to 10 years with a live photo capture during data updates. An actual photograph is required to assure a good performance for face recognition, which is a key biometric authentication method for Digital ID.
- Legal residents are part of the Digital ID ecosystems, and the population database or Digital ID database shall consider their information for the issuance of a Digital ID.
- The Population register should have the possibility to capture and verify a mobile phone number and email address during the registration or update process. Both are used as second-level authentication factors and key for the Digital ID implementation.

1.2 IDENTITY CREDENTIALS

The Digital ID is just one of the identity credentials within the ecosystem of identity credentials issued in a country. This chapter provides an overview of the main identity credentials, their physical formats and security features. Different types of identity credentials are designed for specific use cases, offering advantages for some applications while presenting disadvantages for others.

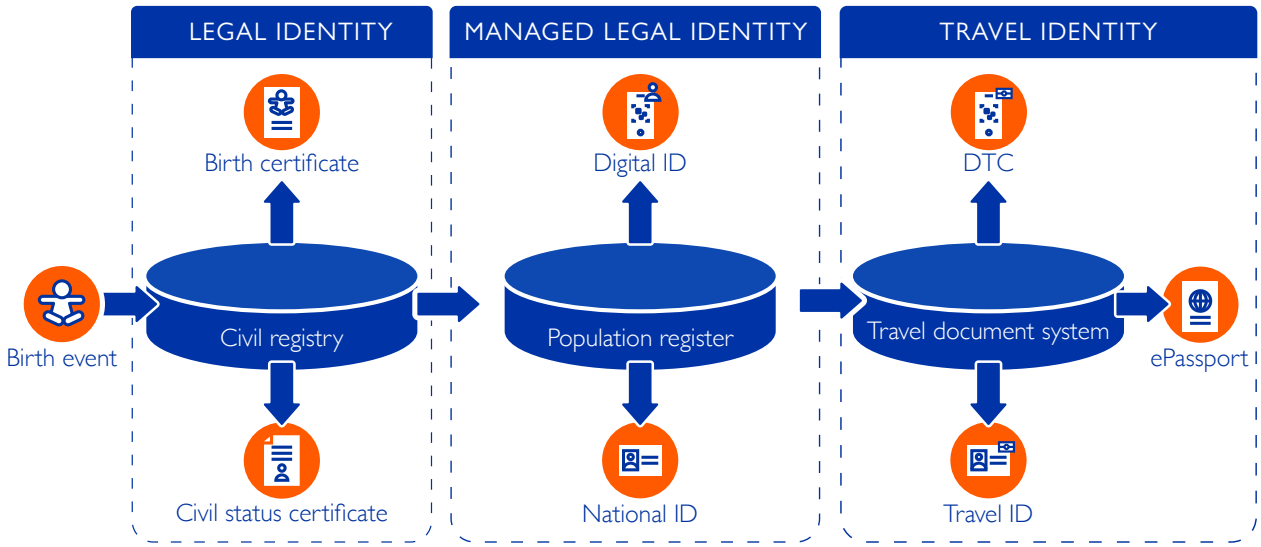
The chapter explains the relationships between these credentials, highlights their common characteristics, and helps classify them according to different use cases. Understanding these credentials is crucial to ensure that each type is promoted for its most suitable use case, thereby avoiding failures in their application.

Identity credentials and issuing systems

The systems responsible for issuing identity credentials include the civil registry, the population register and the travel document issuing system. Each system issues identity credentials for a specific purpose, but all are based on the legal identity registered in the civil registry.

These credentials are issued in various formats, such as paper documents, booklets, cards or digital forms. All credentials share the common feature of reflecting the identity of the bearer in text format. Depending on the type of credential, they may also include additional attributes, biometric information or information related to specific use cases.

Figure 4. Identity credential issuing systems



Grown infrastructure

Many countries have a historically grown infrastructure of travel document issuance, as passports are a requirement for international travelling. The civil registry for the registration of birth also exists in many countries but is not always as common as the systems to issue travel documents.

The implementation of population registers adding biometric information and managing identities and their attributes are growing. As such, the implementation of Digital ID is an opportunity to implement or update the identity management in a country.

1.2.1 IDENTITY CREDENTIAL TYPES AND FORMATS

In the identity management ecosystem, different credential types are issued by different systems. The civil registry issues a birth certificate, which is the initial proof of legal identity after birth registration in the civil registry. Other documents issued by the civil registry are the civil status certificate, showing the actual marital status and for example, possible academic titles.

The population register issues the identity documents and digital credentials representing the legal identity of an individual including the attributes captured in the population register. The main identity credential is issued in the form of a national ID card or as national Digital ID. The national Digital ID is mostly issued as a digital complement of the physical national ID card as both support different use cases.

Identity credential formats

Identity credentials are issued in different formats. From a legacy point of view, the printed credential that has the possibility to add a photograph is the most common in the past. The printed identity information is easy to verify by an inspecting party by manual verification.

To add the possibility of electronic processing, the digital information of the identity is added to the credential. The digital information is either stored in a microchip embedded in the document, like in travel passports or ID cards, or printed in a machine-readable format on the identity credential document.

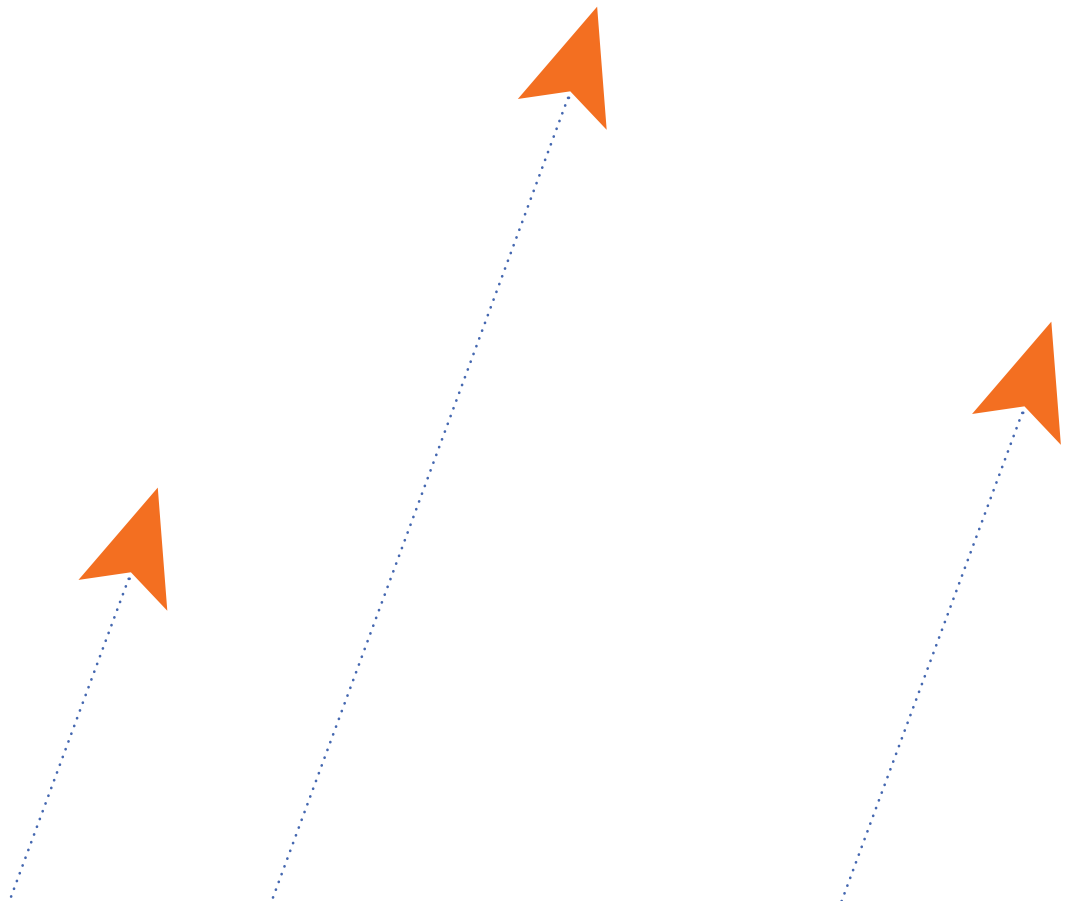


Table 1. Identity credential formats

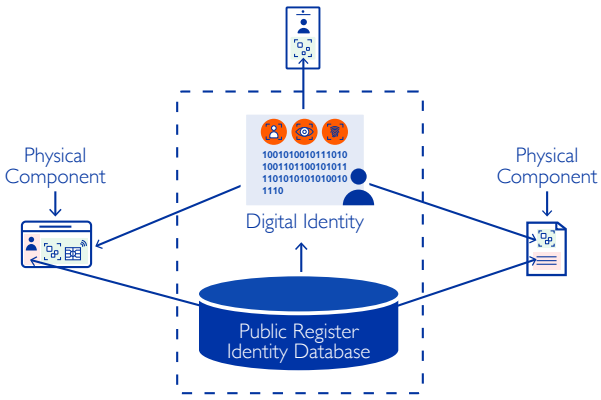
DOCUMENT	PHYSICAL DOCUMENT	DIGITAL COMPONENT	BINDING OF PHYSICAL & DIGITAL
Birth Certificate	Paper document printed without photograph. Possibility to add paper applicable security features against forgery.	The document can have a 2D barcode, for example a QR code containing the digital credential.	The document can have a secure label with electronic chip, binding the digital credential in the 2D barcode to the document.
Civil Status Certificate			
National ID	Physical card with security features.	The card can have a secure chip and/or a 2D barcode containing the digital credential.	The chip in the card can be used to bind the digital credential to the document. The card can have a low-cost security chip to bind a 2D barcode credential to the card.
Travel ID		The card requires a digital credential stored in a chip compliant with the ICAO 9303 specification.	The digital credential of the travel ID is bound to the document/chip by ICAO-specified security mechanisms.
Digital Identity	No physical document.	Digital credential stored on the mobile phone of the user. Digital credential can be presented as 2D barcode or exchanged by Bluetooth transmission.	The digital credential is bound to the user device by security measures provided by the device manufacturer.
Digital Travel ID (DTC)			The DTC is bound to the mobile device od the user and to possibly to the Travel Passport of the user, depending on the ICAO DTC type used.
Travel Passport	Physical Booklet with data page and visa pages.	The passport can have a secure chip and additionally a 2D barcode containing the digital credential.	The digital credential of the passport is bound to the document/chip by ICAO-specified security mechanisms.

For example, on electronic passports, some information is printed in the machine-readable zone in characters which are optically easily readable, but which contains only a very low volume of data. The most common format of printing machine-readable information is a 2D barcode, like the QR code. The QR code can be easily read by almost all electronic devices that have a camera, which reduces the cost of infrastructure. The QR code is only an optical representation of digital data, which could also be stored in a database or in an electronic ID card or e-passport chip. Some systems refer to the digital data component as the virtual component of the identity credential. The limitation of a QR code is the amount of data (~3 kilobytes), depending on other technical factors like error correction. Electronic chips in documents can store more information, usually between 16 and more than 500 kilobytes, while databases and mobile devices provide much more memory than this range.

The digital representation of the identity information can be referred to as a digital credential that can be used as only digital information or in combination with a physical document (printed as 2-dimensional barcode or stored in a microchip embedded in the document). Digital credentials are the bases of a Digital Identity, a form of digital credential bound to a mobile device for usage in digital transactions or presentation as digital identity credential from a mobile wallet.

The digital credential (digital component) of an identity document can be used in digital format as data and can be bound to a physical document. The process of binding a document to a physical component is performed by different measures and allows to identify a physical document by its digital credential. By using a document binding mechanism, the verifier can check if the digital credential presented belongs to the physical document. The binding creates the factor of originality, meaning to identify the original document versus a digital copy of the digital credential. For some verifications, this binding of a digital credential to a physical credential is required. The travel passport is one example, where the use case requires verifying that a traveller has the original passport presented at the border control. The requirement to verify an original document versus the verification of only the digital credentials depends on the use case.

Figure 5. Components of a document



Binding of identity data to identity credentials

Identity data can exist independently or be linked to physical media such as a document, chip, booklet or mobile phone. This process, known as binding, establishes a fixed link that allows external entities to verify the authenticity of the physical document. The technical methods used for binding depend on the type of media. For example, a passport photo in a travel document is secured with a hologram overlay to ensure it has not been tampered with. Verification requires knowledge and tools to check these security features.

Traditional security features on paper documents serve two purposes: protecting identity information from forgery and proving the document's authenticity. When a document includes a photograph, the verifier must manually confirm the identity of the bearer. While physical security features enhance document integrity, they can be costly and challenging to process. Verification of printed identity documents also depends on the verifier's expertise.

Security of credentials

The security measures for physical and digital credentials follow the same security principles:

- **Integrity**

  The credential's information is protected and integrity is verifiable.

- **Authenticity**

  Credentials are verifiable as authentic and the issuer can be identified securely.

- **Confidentiality**

  Information of the credential can be secured against unauthorized access.

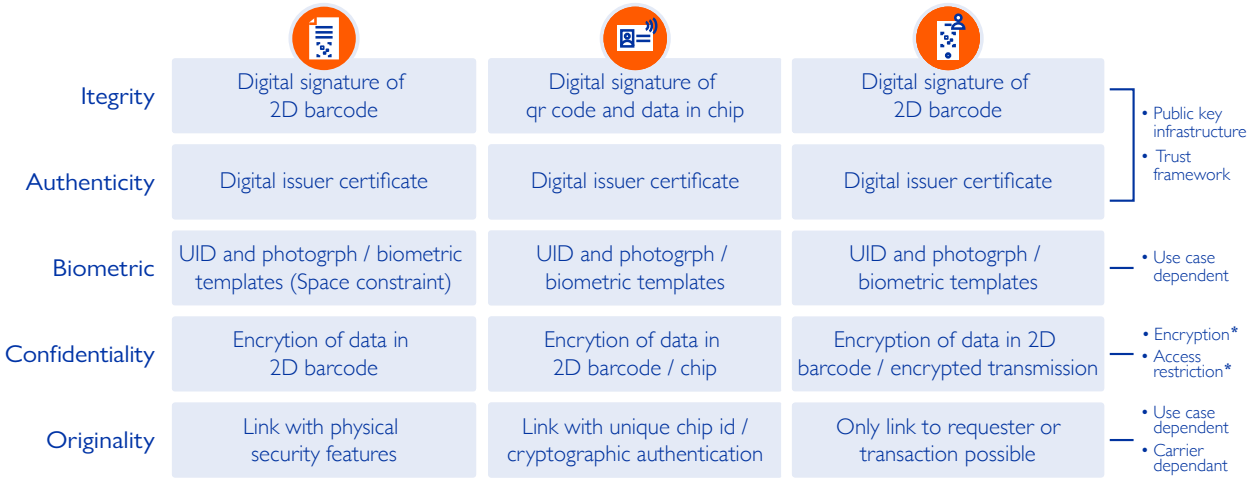
- **Originality**

  The credential can be identified as original, bound to a physical token.

- **Biometric**

  Biometric link of the credential to the owner.

Figure 6. Security of credentials



* Complex due to technical crytographic requirements on verifier side

The implementation of security measures varies based on the type of credential, with each type offering specific mechanisms to achieve the desired level of security. The security level required depends on the use case and the verifier's tools or knowledge needed to check the credential's security.

Binding physical and digital credentials together provides a higher security level than using either alone. However, the security level should align with the use case, as higher security can involve greater costs and may not always be necessary. For instance, verifying identity information may not require an original document, while registering a marriage might necessitate an original birth certificate. The choice of credential types should balance security and usability according to the planned processes.

Incorporating digital credentials such as digital IDs or combined credentials, is recommended. Digital credentials enable easy electronic verification, reducing the reliance on specialized knowledge needed for physical credential verification. Combining digital and physical credentials supports both automated and manual verification.

The classification and evaluation assume that credentials are implemented correctly and leverage the best available technologies.

Table 2. Security categorization of credentials

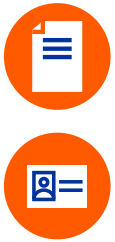
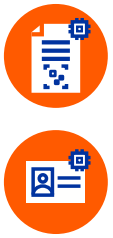
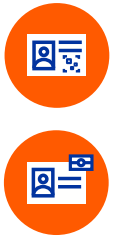
CREDENTIAL TYPE	INTEGRITY	AUTHENTICITY	CONFIDENTIALITY	ORIGINALITY	BIOMETRIC	COST
 Digital Credential as 2D Barcode	HIGH	HIGH	LOW MEDIUM if encrypted, (static)	LOW Can be copied	MEDIUM with low-resolution photo HIGH Template-based biometric (Finger/Iris)	LOW
 Digital Credential as Data Token	HIGH	HIGH	LOW HIGH if encrypted (dynamic)	LOW Can be copied	HIGH Template-based biometric (Finger/Iris) Full photo for face recognition	LOW
 Digital ID	HIGH	HIGH	LOW HIGH if encrypted (dynamic)	LOW HIGH, if mechanism to check the device	HIGH Mainly face biometric	MEDIUM
 Document Paper / Card	LOW MEDIUM if protected with physical security features	LOW MEDIUM If verifier is knowledgeable	LOW knowledgeable	LOW MEDIUM if verifier is knowledgeable	LOW Only secured photo	LOW MEDIUM with security features
 Document and Digital Credential	HIGH	HIGH	LOW MEDIUM if encrypted, (static)	LOW MEDIUM if verifier is knowledgeable	MEDIUM with low-resolution photo HIGH Template-based biometric (Finger/Iris)	LOW

Table 2. Security categorization of credentials (continued)

CREDENTIAL TYPE	INTEGRITY	AUTHENTICITY	CONFIDENTIALITY	ORIGINALITY	BIOMETRIC	COST
 Document Paper / Card and Digital Credentials 2D Barcode with NFC Token	HIGH	HIGH	LOW MEDIUM if encrypted, (static)	HIGH	MEDIUM with low-resolution photo HIGH Template based biometric (finger/iris)	MEDIUM
 SmartChip ID / SmartLable with Digital Credential in Chip and 2D Barcode	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
 National-ID with Travel ID (ICAO Standard) Or Travel ID Only (ICAO Standard)	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
 Travel Passport (ICAO Standard)	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
 Digital Travel ID (ICAO DTC)	HIGH	HIGH	LOW HIGH if secured usage	LOW HIGH if mechanism to check the device	HIGH Mainly face biometric	MEDIUM

1.2.2 DIGITAL CREDENTIALS

Digital credentials, often called verifiable credentials (VC), consist of identity claims digitally signed by the credential issuer. While anyone can issue a verifiable credential, the verifier must trust the issuer. The subject of a digital credential can be an identity, a document linked to an identity or even an asset, such as a vehicle certificate certifying the existence of a vehicle. These credentials are also used for dematerializing and securing documents or proofs of transactions, following the same principles but with different subjects.

In the context of digital identity, as described in this toolkit, a digital credential always pertains to an individual identity and is issued by a government authority. Digital credentials can take various formats and align with either a generic trust framework or a use case-specific trust framework, such as the ICAO framework for travel documents.

A digital credential's key components are defined by the credential issuance policy and the individual for whom it is issued. These components include essential information categories derived from the issuer's database or related to the credential's issuance.

Table 3. Digital credentials (verifiable credentials) content

ELEMENT	DESCRIPTION	ORIGINATION
Type	Categorization of the credential type or use case. Types can be defined by an issuer or a standard. Type could be a national-ID credential, student ID, driver's license or any other.	Defined by the framework policy and set by the issuer.
Issue timestamp	Is the date and time when the issuer has issued the credential technically.	
Validity timestamp	Validity refers to the time period during which the credential remains valid, defined by a start and end date. If the validity only specifies an expiry date, the issuance timestamp typically serves as the start of the validity period.	Defined based on the credential type policy in relation to the subject (individual) eligibility or request.
Subject Information	In the case of a digital identity credential, the subject refers to the identity information of the individual to whom the credential is issued.	Database of the issuer.
Subject Attributes	Any attribute related to the subject the issuer adds. Attributes can be person related.	Database of the issuer.
Type attributes	Attributes are details added by the issuer based on the individual's request or eligibility under the policy governing the credential issuance. For instance, a retirement date is determined by the retirement policy and calculated accordingly; it is not part of the individual's personal information but rather linked to their eligibility and the policy criteria.	Issuance policy related to the credential type.
Token binding	Token binding applies only when the credential is linked to a physical token, such as an ID card, chip, or mobile phone.	Generated during the issuance process and related to the individual physical token on which the digital credential is stored.
Origination Proof	Serves as proof of the issuer's authenticity, which can be electronically verified by anyone.	The issuer's signing certificate, endorsed by the issuing authority, is trusted by the highest authority within the trust framework.
Integrity Proof	Proof of the credential's data integrity ensures that, at the time of verification, the credential has not been altered or falsified and that the information remains consistent.	Generated cryptographically with the digital signature during the credential issuing process.

A digital credential is a data container secured against manipulation through a digital signature, aligned with the trust framework's policy. It can be stored in a database, chip or 2D barcode and allows for automatic processing and verification.

Digital Seals / Visible Digital Seals (VDS)

The principle of a digital credential is universal but may have different names depending on regional conventions. Under the European eIDAS framework (electronic identification, authentication and trust services), it is referred to as a digital seal, which involves sealing data with an electronic signature under the eIDAS trust framework. When displayed visibly, it is often called a VDS or a VC.

Digital Credential Data Formats

The digital credential's data content, or payload, must be packaged into a specific format, referred to as a digital token format. Various standardized formats for digital credentials include:

- **ISO-22376:** VDS standard for documents and credentials;[6]
- **ICAO-9303 Part 13:** VDS standard for travel-related documents;[7]
- **W3C Verifiable Credentials Data Model:** Standard by the World Wide Web Consortium;[8]
- **ISO-18013:** Mobile driver's license (mDL).[9]

Some formats, such as the mobile driver's license (mDL) and ICAO VDS, are optimized for specific use cases, while others, like ISO-22376 and W3C, are more generically defined.

Once the digital credential is structured into a compliant digital token format, it can be digitally processed, stored or visualized as a 2D barcode.

1.2.3 TRAVEL IDENTITY DOCUMENTS / TRAVEL CREDENTIALS

The travel document system connects to the population register to ensure a validated unique identity. The system issues internationally recognized travel documents and digital travel credentials in compliance with ICAO standards. ICAO, a United Nations suborganization, operates under the Chicago Convention of 1944 to facilitate international travel among Member States. The ICAO TRIP (Traveller Identification Programme) Strategy, rooted in Annex 9 of the Chicago Convention, includes initiatives to standardize travel documents for interoperability in border control processes.

The ICAO-9303 document specifies the technical standards for physical and digital travel credentials, including visual and electronic travel documents, crew member certificates, visas and travel ID cards. To ensure the integrity and authenticity of digital travel document data, ICAO Member States have established the ICAO–PKD,[10] a trust framework based on public key infrastructure. The ICAO–PKD enables secure verification of data authenticity, integrity and origin, and is governed by participating Member States and administered by ICAO.

Limitations of travel documents

Travel documents and their digital credentials are based on the legal identity recorded in a population register, with issuance relying on the guaranteed uniqueness of each identity. The identity data in travel documents is optimized for international travel and border control, following an established infrastructure dating back to the introduction of machine-readable passports in the 1980s and electronic passports in 1998.

6 ISO, Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object (ISO, 2023).

7 ICAO, Doc 9303, Machine Readable Travel Documents (ICAO, 2021).

8 Manu Sporny, Dave Longley, David Chadwick, Orie Steele, Verifiable Credentials Data Model v2.0 (The World Wide Web Consortium, 2024).

9 ISO, ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application (ISO, 2021).

10 ICAO, The ICAO Public Key Directory (PKD) (ICAO, n.d.).

Legal identities in population registers often use local alphabets, posing challenges for immigration and border control. To ensure interoperability, travel identities are transliterated into Latin characters. However, inconsistent and undefined bidirectional transliteration between languages can result in varying name representations. The standardized machine-readable identity information on travel documents and electronic chips uses Latin characters exclusively, as defined by ICAO specifications. While this normalization facilitates international travel, challenges persist when using travel identity documents for other purposes.

1.2.4 CHALLENGE FOR DIGITAL IDENTITY CREDENTIALS AND DOCUMENTS

The identity document ecosystem, encompassing both digital identities for travelling (DTCI)[11] and legal identities, as well as the issuance of travel ID cards and national ID cards, may appear redundant and costly. While combining these credentials into one may seem logical, practical and operational challenges remain.

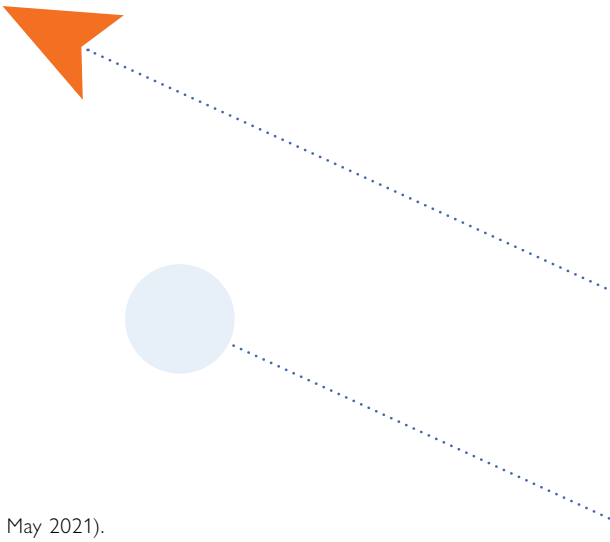
Issuing two distinct digital identity credentials – one for travelling under ICAO standards and another for legal identity – from a single digital identity system is technically feasible and cost-effective. Once implemented, issuing these digital credentials electronically becomes efficient. Both credentials can be stored on the same mobile device, allowing practical use depending on the requirements of each use case.

A significant challenge is managing two separate trust frameworks. The travel ecosystem follows international ICAO policies, while legal identity systems adhere to local laws and regulations. In some countries, these document types are issued by different authorities, adding political and administrative complexity. Similar issues arose with digital COVID-19 vaccination certificates, where varying trust frameworks led to international incompatibilities.

The feasibility of combining a travel ID and national ID into one physical card depends on the country's use cases. ICAO standards for travel IDs impose specific features such as enhanced physical security and large chip capacity, which may increase manufacturing costs and may not be necessary for a national ID. The chip must store two distinct digital credentials since the mandatory data set for a travel ID differs from that of a legal identity, following separate policies and trust frameworks.

Countries must carefully evaluate the necessity and benefits of issuing travel IDs to avoid unnecessary costs for citizens. A national ID should be mandatory, ensuring equal access to government services, identity proof and societal participation. It should be affordable or subsidized. Travel identity documents, such as travel IDs or passports, are optional and limited to cross-border travel. Unlike passports, travel IDs are not recognized under the Chicago Convention and are valid only in regions with bilateral agreements or special zones like the European Union.

Digital IDs present an opportunity to streamline processes. A digital identity system designed for general identity issuance can also issue ICAO-compliant DTC. Countries could adopt digital identities for travel, reducing reliance on ICAO-compliant physical ID cards and lowering total costs. This approach allows countries to design their national IDs based on specific needs, minimizing expenses for citizens while maintaining functionality for travel-related use cases.

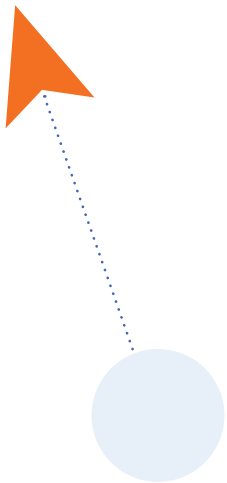


11 R. Rajeshkumar, Digital Travel Credentials (ICAO, Montreal, TRIP Symposium, 25–28 May 2021).

Digital ID as opportunity for travel ID

A travel ID may not be practical if the number of bilateral agreements enabling its use does not justify the cost for citizens. Nonetheless, some countries choose to issue a combined travel ID and national ID in one physical card, citing potential future use. However, such future use is often uncertain, and the significant cost difference between issuing a travel ID versus a national ID under local policy could result in wasted investment.

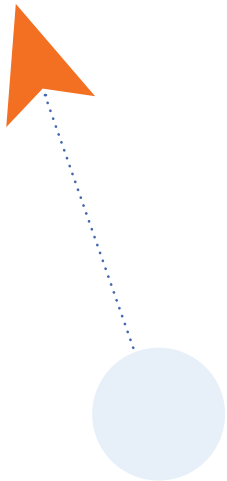
The infrastructure required for a national Digital ID is very similar to that needed for a DTC (digital travel ID as per ICAO standards). By first implementing a national Digital ID, a country can later add functionality for a DTC without incurring upfront costs for both systems. Using a digital credential for travel or extending the functionality of an existing national Digital ID for travel purposes is a more cost-effective and beneficial solution for citizens, as travelling with a travel ID requires separate State agreements.



1.2.5 TAKEAWAY AND SUMMARY

Digital credentials form the foundation of secure identity management systems and the issuance of identity documents containing digital credentials. These credentials are integral to digital identities, managed and utilized within a digital ecosystem. They can take various formats and have the following characteristics:

- Digital credentials include identity data, attributes, issuance-related information and use-case-specific or eligibility details based on the policy governing their issuance.
- Each credential issuance adheres to a policy and trust framework, which can be generic or specific to a use case, such as travel documents.
- Different types of identity documents and digital credentials are designed to serve specific use cases, offering distinct advantages.
- Thorough analysis of use cases and processes is essential to select and design the optimal set of identity credentials for the intended implementation.
- Various digital credential formats exist, and a digital identity system can manage multiple formats to support diverse applications and use cases on a single platform. However, managing different trust frameworks remains a challenge.



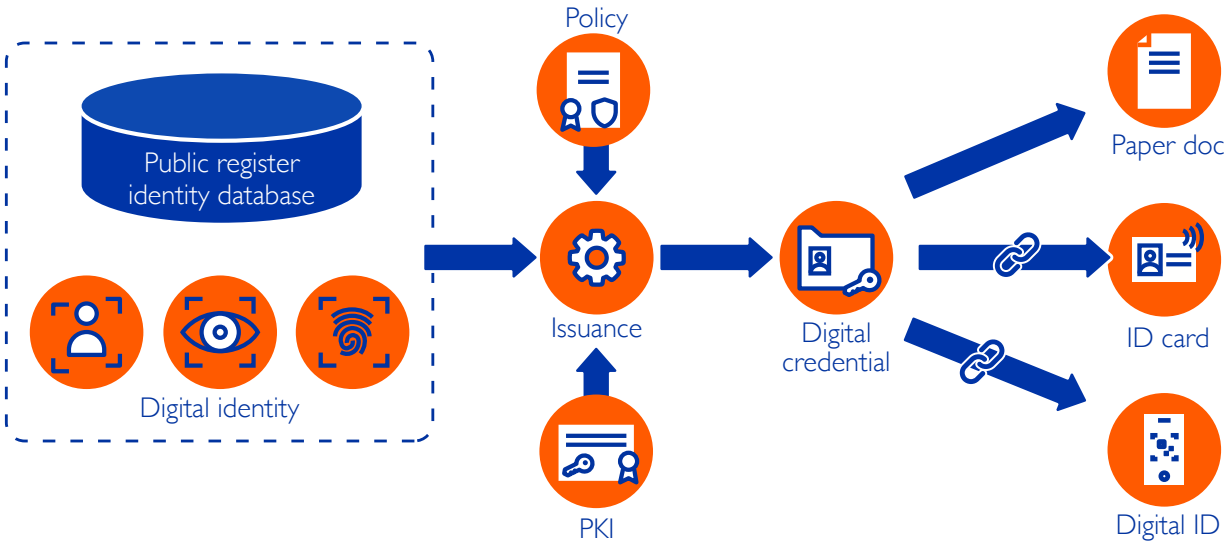
1.3 UNDERSTANDING OF DIGITAL IDENTITY

Digital identity is commonly defined as a data set created by an authority that links an individual's legal identity with their biometric data. This data set, representing the individual's digital identity, is stored in a secure database, such as a population register, and requires robust measures to ensure privacy and protection against manipulation or theft. To make this digital identity functional for various use cases, it must be extracted from the secure database and safeguarded with additional security measures for use in different applications.

Historically, identity information was printed on secure documents, but this approach has limitations in terms of automation and security. A more advanced method involves issuing digital identity credentials under a policy framework defined by the issuing authority. These credentials can be stored and used in various formats, such as ID card chips, electronic passports or 2D barcodes.

Verifying digital identity requires a technical infrastructure capable of reading the credentials and accessing a trust framework to confirm their integrity and origin. While the principles governing the use of digital identity remain consistent, the usability of these credentials depends on the trust frameworks and media formats employed. For example, an electronic passport stores digital identity information on its chip, which is optimized for border control but may not be suitable for other applications.

Figure 7. Digital identity issuance



When digital identity credentials are used solely in digital form without a physical counterpart, they are referred to as Digital IDs. These credentials are stored securely in a digital wallet on the owner's mobile device. During the issuance process, the credential is bound to the specific device, ensuring it cannot be used on unauthorized devices.

Mobile operating systems offer standard wallet applications managed under the policies of private commercial entities. These wallets can store various credentials from different trust frameworks, making them suitable for commercial applications. However, for government-issued Digital IDs, such dependencies on private entities pose challenges to government sovereignty and control.

Governments typically develop and manage Digital ID applications under their own policies, ensuring control over functionality and enabling the gradual addition of new services via updates. Governments may license software from private vendors or use open-source Digital ID applications. Open-source solutions provide flexibility and cost savings but require local expertise for customization and maintenance.

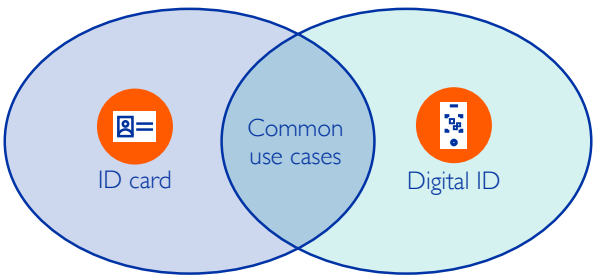
The downside of commercial licensing is a dependency on a specific vendor, along with their capability and willingness to implement features. This dependency can be costly for countries and limit flexibility. Open-source Digital ID applications, by contrast, allow countries to modify and improve the software as needed, and they can be used license-free.

Digital ID systems support a wide range of use cases, contributing significantly to a country's digitalization and offering benefits to the population. Unlike physical smartcards, Digital IDs in mobile applications provide seamless integration into digital services and accessibility for citizens abroad. Once enrolled, citizens can remotely access government services, enhancing inclusivity and convenience.

Coexistence of Digital id and physical identity credentialss

A Digital ID and its use on a smartphone are not expected to replace the physical ID card. Instead, the two will coexist and complement each other, as each is optimized for different use cases with some overlap in functionality. By combining a physical ID with a Digital ID on a mobile device, the range of possible use cases for individuals and governments is expanded, benefiting all parties. Over time, certain functions of the physical ID card may migrate to the Digital ID, potentially reducing the cost of producing physical ID cards.

Figure 8. Digital ID and ID card coexistence



Updating the smart chips on physical ID cards to enhance digital functionality is more complex compared to extending the capabilities of a Digital ID within a digital ecosystem, which can be done through online updates and applications. This makes Digital IDs more adaptable and easier to evolve.

Despite this, physical ID cards remain essential as tangible documents that can be used anytime, even without electricity or internet connectivity. They provide proof of physical possession and serve as a secure token containing both printed and digital identity information. Physical IDs also play a crucial role in certain use cases requiring in-person presence. For example, physical IDs are often required during enrollment for a Digital ID to ensure additional consent and validation before installing the Digital ID on a mobile device. This added layer of security enhances transactions and processes that demand physical verification.

Role of smartphones

Smartphones are central to Digital ID systems as highly personal devices under user control. They have become essential for numerous applications increasingly optimized for mobile use. In this context, the term "mobile phone" specifically refers to smartphones.

Compared to personal computers, smartphones offer several advantages for everyday transactions. They combine multiple technical functions, including cameras, near field communication (NFC) for reading smart cards and Bluetooth for proximity communication, making them more convenient for users. These features enable tasks such as taking photos, biometric face recognition and reading digital credentials in 2D barcode formats. Over the past decade, smartphone penetration has significantly increased, reaching levels sufficient in most regions to support the implementation of mobile services.

Digital services are progressively migrating to smartphones, as seen in the banking sector. Transactions are often conducted via smartphone wallets or QR codes, with traditional cards gradually becoming backup solutions for cases where phone-based payments are unavailable. The banking sector, driven by commercial goals and customer satisfaction, has been a digital service pioneer, setting a precedent for government digitalization. Banking services, which require high levels

of security, fraud prevention and user accessibility, share similar attributes with government identity services. Technologies such as two-factor authentication, already widely used in mobile banking, demonstrate feasibility and readiness for broader applications.

A key success factor for digital services, including Digital IDs, is ensuring usability and providing adequate user education for handling digital applications. This fosters adoption and satisfaction, supporting the broader digital transformation.

Security threats to digital services

Credit card fraud is most prevalent in regions where payments can be executed using only the credit card number, often due to regular online transactions lacking additional security measures. Such fraud is mitigated by implementing robust security mechanisms, as seen in mobile payments. Credit card companies have significantly reduced fraud by adopting transaction confirmation via messages, digital apps and two-factor authentication to secure approval from the card owner.

A major threat to digital services, including banking and identity systems, is phishing and social engineering attacks. Phishing attacks involve fraudsters sending deceptive emails encouraging victims to click infected links. These links install malware on the victim's device, allowing attackers to spy on passwords or transaction codes. Attackers often attempt to register stolen credit cards on smartphones or hijack digital banking accounts. Preventing such fraud requires user education and the use of secure communication channels. Many banks now communicate exclusively through their secure apps and inform customers that official communication will not occur via unsolicited emails.

Social engineering attacks involve gaining personal knowledge about a victim and using it during a call to manipulate or intimidate them into revealing sensitive information, such as PINs or banking credentials. Attackers may impersonate authorities such as police, government officials or central banks to create a sense of urgency or fear. Combating these attacks relies on user awareness, education and consistent warnings about such tactics.

1.3.1 FUNCTIONALITY OF DIGITAL ID APPLICATIONS

The use cases outlined in this toolkit represent the most common applications where Digital IDs can support a country's digitalization efforts. While these are the primary examples, many additional use cases can be developed as digital applications are tailored and expanded based on specific needs and capabilities.

The most important use cases revolve around six core functionalities of a Digital ID and its related systems. These functionalities are centred on digital identity and are delivered to citizens through dedicated mobile and web applications. Service providers integrate some of these functionalities to enhance their online services by enabling the use of digital identities, while other functionalities ensure the maintenance and security of the Digital ID system for users.

Key benefits of Digital IDs include the elimination of paper documents, optimization of online services, and 24/7 accessibility to government services from anywhere. Reducing paper and physical processes lowers costs in the medium and long term for governments while enhancing convenience for citizens through extended availability and simplified access.

The core functionality of Digital ID applications

1. Single Sing On
2. Transaction approvals
3. Digital ID web portal: Allows users to manage digital devices and control their identity.
4. Issuance of Digital ID passes or VCs: Supports multiple purposes.
5. Digital electronic signature: Enables secure signing by citizens.
6. Digital mailbox: Facilitates secure communication between the Government and citizens.
7. Document exchange: Enables secure sharing of documents.
8. Validated ID token

While functionalities 5, 6 and 7 are not direct uses of Digital ID, they are enabled by it. These functions require user authentication, a secure environment within a government-controlled application and a confirmed Digital ID for execution. By installing the Digital ID application on citizens' phones, the Government creates a universal service window for identity-related core services. This approach provides access to certain applications without requiring citizens to use multiple separate apps.

However, a Digital ID application cannot replace applications or services provided by entities other than the identity provider. Instead, it serves as a platform to bundle generic services related to core identity, streamlining access for citizens.

Onboarding

Before using a Digital ID application, users must complete an onboarding process after installing the mobile app. During onboarding, users identify themselves using a unique identifier, such as a UID, email or another identifier linked to the identity management system. The process typically includes biometric verification, where a live photo of the user is compared with the one stored in the identity management database to ensure the user is a live person and not a photographic image.

User authentication during onboarding is the most critical step, as it installs the Digital ID on the user's smartphone and links the device and user identity to the data and profile in the population register. Some countries require this process to be performed in the presence of a government officer, while others only require confirmation of additional information, such as a verified telephone number or email.

Additionally, the user must confirm their mobile number and email through two-factor authentication (2FA). For security purposes and to minimize fraud, the email address and mobile number are retrieved from the identity management system. The user receives a verification code via SMS and email, which they must confirm. Once all authentication steps are successfully completed, the Digital ID app and the user's identity are securely linked to the mobile device, enabling its use.

Authentication levels

During the onboarding process, the user is required to authenticate their identity. Depending on the application and local circumstances, the authentication level of the user's identity may vary. For example, a user who onboards by providing their national ID number, email and phone number has a low authentication assurance level. If the user undergoes biometric verification, the assurance level increases. Furthermore, if the user is authenticated in person by an official at an enrolment office, the authentication assurance level for the identity becomes even higher. Linking requested services to a specific authentication level is possible. For instance, a legal digital signature typically requires the highest level of authentication.

Authentication levels can be categorized with names such as bronze, silver and gold or with stars, such as 1-Star, 2-Star or 3-Star authentication levels. If a user attempts to access a service with an authentication level lower than what is required, the service is rejected.

A tiered level system allows for an easy onboarding process at a lower authentication level, enabling access to basic services that encourage user engagement. Over time, users can be motivated to authenticate at a higher level to access more secure and advanced services.

1.3.1.1 SINGLE SIGN ON

The Single Sign-On (SSO) functionality enables users to access multiple government portals using their Digital ID through a single mobile application. Various government organizations offer services via dedicated portals, which may be unified under a central government service window or operated separately for different administrative regions within the country. Regardless of the setup, SSO simplifies access to multiple portals managed by different government entities.

SSO functionality often allows users to log in using biometric authentication, eliminating the need to remember passwords. This technology reduces costs associated with password resets, prevents misuse of insecure passwords and enhances overall security and accessibility to government services. SSO is a critical feature of the Digital ID ecosystem.

When a user logs in to a government portal, the portal redirects the login request to a central authentication gateway. The user must first be onboarded with their mobile device, and the gateway sends a login request approval to the user's mobile device. Once the user confirms the login request on their device and is authenticated, for example, through biometric face recognition, the gateway issues a secure login token to the application the user wishes to access. This token can be used for the entire session, including interactions with multiple applications.

With SSO, users have a single point and method for signing in through the identity gateway managed by the central SSO system.

Identity theft

Digital systems have become highly secure, making social engineering the primary threat to Digital ID theft, as discussed in Section 1.3. Criminals often attempt to deceive victims into sharing security codes received via email or SMS, enabling them to install the victim's digital identity on their own device. This tactic mirrors methods commonly used in digital crimes to take over bank accounts or steal funds.

The key to combating such threats lies in continuous communication through the Digital ID application, public media or the Digital ID web portal. These channels help ensure that users remain aware of potential risks and understand how to protect themselves.

1.3.1.2 TRANSACTION APPROVALS

The same methodology and process used for SSO are applied to approve transactions performed online by the user. During the confirmation process, the user is typically shown which application is requesting transaction approval, allowing them to verify that the request was initiated by their action and not by a fraudster.

App-to-app Digital ID functionality

If a user initiates a login or transaction request from another government application on the same mobile device as the Digital ID app, the two apps can communicate through an app-to-app channel. Modern smartphone operating systems support app-to-app communication, enabling one application to link directly to another.

For the user, this process appears seamless. When a login request is initiated from a government app, the Digital ID app automatically opens for authentication. After successful authentication in the Digital ID app, the system switches back to the original government service app. This process is designed to be smooth and user-friendly, regardless of the underlying IT infrastructure and communication involved in the application switch.

This method facilitates the use of the Digital ID app and government service apps on the same smart device, providing a convenient and efficient experience for the user.

1.3.1.3 DIGITAL ID WEB PORTAL

The Digital ID web portal is a centrally managed application within the Digital ID system infrastructure, designed to allow users to manage their Digital ID without relying solely on a mobile device. Users can log in via SSO using the Digital ID mobile app or through traditional two-factor authentication methods, such as SMS or email codes. If access credentials, a mobile device with the Digital ID or passwords are lost, the web portal enables users to remotely delete the Digital ID from the lost device or reset identity-related parameters.

For systems supporting digital signatures, the portal provides access to signature functionality through a web interface, enhancing convenience for users working on PCs. While digital documents like PDFs can be signed using mobile devices, the portal simplifies the process for documents typically created on a computer. Authentication for digital signatures depends on local digital signature laws and policies and may include password-based authentication, integration with the mobile Digital ID app or biometric methods.

The web portal can also serve as a general service hub for the entity managing the Digital ID, offering additional services beyond those available in the mobile app. If the same entity manages physical ID documents, such as cards or certificates, the portal can act as a gateway for those requests as well.

Core functionalities such as a digital mailbox for government-citizen communication and the exchange of government-issued documents, can also be integrated into the portal. These features support digital transactions that may be more convenient on a PC than on a mobile device, further enhancing the system's utility and user experience.

1.3.1.4 ISSUANCE OF DIGITAL ID PASSES FOR MULTIPLE PURPOSES (WALLET CREDENTIALS)

The issuance of Digital ID passes allows for the creation of offline and online usable digital credentials stored in the wallet of the Digital ID app. The primary Digital ID, such as a national ID, can also be issued as a pass within the wallet, containing only the holder's identity information. Additional passes or credentials issued to the wallet may include identity information combined with other attributes or details provided by another entity, often a government agency.

Digital ID passes can be presented digitally as VDS and verified both offline and online using the Digital ID app. The app includes a verification function for passes and also allows them to be used as digital tokens directly on websites, expanding their functionality and convenience.

Example for wallet passes

Digital ID wallets can generate passes for various use cases, functioning as (VCs) in barcode format or as digital tokens. While the potential applications are extensive and depend on the specific needs of governments, citizens and countries, the following key use cases illustrate common examples.

- Pension pass to proof the pension eligibility and live check;
- Health pass for access to health services indicating the eligibility of health insurance;
- Vaccination pass (for example COVID-19 vaccination certificate);
- Student pass;
- Insurance pass and proof;
- Driver's license;
- Vehicle license;
- Medical ID for health workers (doctors / nurses).

1.3.1.5 DIGITAL ELECTRONIC SIGNATURE FOR CITIZENS

A digital signature is an optional feature that enables secure and authentic user signatures for interactions with governments or other accepting parties. Similar to how governments sign electronic passes and documents to verify their origin and authenticity, a user's digital signature employs the same technology to provide proof of authenticity for documents or transactions.

Digital signatures on documents involve the user signing a PDF or similar file with a personal key issued by a public key infrastructure (PKI). A digitally signed document cannot be altered, and any manipulation or falsification is detectable. This process secures documents by ensuring their integrity and verifying their origin through the digital certificate and keys used during signing. The signing process adheres to cryptographic industry standards, commonly applied to PDF documents, where the signature can be validated using standard PDF readers.

To perform a digital signature, the user requires a personal digital certificate, and cryptographic keys issued specifically to them. These credentials are secured to ensure that only the rightful owner can use them. A specialized PKI is often established to issue citizen signature certificates. Secure timestamping is also incorporated to record the exact time of the signature. During the signing process, the user must authenticate and confirm their identity, typically using methods defined by national digital signature laws, such as authentication through a Digital ID application.

Implementing digital signatures requires a regulatory framework and supporting legislation in the country. Such legislation must equate the legal validity of digital signatures with handwritten ones to encourage digital transformation. This framework is typically supported by policies, stringent security requirements and an audit mechanism. Digital signature systems demand robust regulation, monitoring and auditing by the relevant authority.

In the European Union, digital signatures are governed by the eIDAS regulation, which provides a comprehensive legislative framework for trust services and digital signatures. Countries outside of the Euroepan Union often face challenges in defining and auditing their digital signature frameworks to ensure compliance and security.

Integration of signature in Digital ID

Digital signatures have been available for many years, with the European Union establishing its first digital signature law in 1999. However, early implementations were not widely adopted due to significant security requirements that made their use cumbersome and costly. Users needed a smartcard, a smartcard reader and specialized software installed on their PCs. Frequent IT advancements required constant updates, making the solution challenging to maintain. A major limitation was the need for users to securely store and manage their private keys, often on smartcards or mobile SIM cards, which proved impractical.

Modern solutions have addressed these challenges through remote signing technology. In this approach, users' private keys are securely stored in centrally managed hardware security modules (HSMs), purpose-built for this task. These keys can only be accessed with user authentication via their Digital ID and an additional security component integrated into the secure Digital ID application. Remote signing offers greater convenience, allowing users to switch devices easily and perform digital signatures from both web portals and mobile devices.

Despite its technical advancements, widespread adoption of digital signatures by citizens can take years, requiring robust communication and user education efforts. Once established, digital signatures transform a country's digital ecosystem, enabling fully paperless services. They eliminate the need for physical documentation or applications, bridging the gap in digital service delivery and elevating the efficiency and accessibility of government and private sector interactions.

Process of digital signing

To perform a digital signature, the user selects a stored PDF document, such as an application form or any other created PDF. Before signing, the user must confirm they are familiar with the document's content and provide full consent to sign it. Once confirmed, the signing process is initiated and completed either on the server (remote signing) or directly on the mobile phone using the device's secure components.

Digital signature functionality is often extended to a web-based application accessible from any personal computer. Since most documents are created on computers, the Digital ID web portal enables document signing in a user-friendly environment. While the web portal offers a more comfortable interface with larger screens for document readability and confirmation, the security and user authentication for signing rely on the Digital ID app.

The digital signature feature enhances the Digital ID ecosystem by providing users with a secure way to sign electronic documents. It facilitates document submission to government entities or use in private business transactions, enabling seamless, end-to-end digital service delivery across all sectors.

1.3.1.6 DIGITAL ID MAILBOX FOR THE GOVERNMENT-TO-CITIZEN COMMUNICATION

The operation of a Digital ID mailbox can significantly enhance the security of the Digital ID ecosystem. While users commonly use their private email addresses for communication with the Government, including for Digital ID enrollment, this is considered secure as the email is privately owned and suitable for two-factor authentication. However, relying on private email addresses for ongoing communication has certain limitations.

- **Security**

  Communication through private email is not inherently secure, posing a risk when exchanging personal information and sensitive documents. Private email providers are more susceptible to threats, which could lead to identity theft or unauthorized disclosure of personal information contained in government documents.

- **Trust**

  Another issue is verifying the authenticity of communication. Phishing attacks, where criminals impersonate government agencies in emails

to deceive users into clicking malicious links, are a significant threat. These links can lead to cyberattacks, potentially compromising an entire computer. Identifying fraudulent emails designed to look like official government communication can be challenging for users.

- **Registered communication**

  Users may change email addresses or claim that an email or communication was lost, especially in cases such as missed submission deadlines. While the traditional postal system offers registered mail services, including unattended delivery to a registered physical address, verifying claims of lost emails is challenging. This makes standard digital mail channels unsuitable for certain types of critical communications.

The solution to address these challenges in digital transactions is the introduction of a digital official mailbox, a registered mail address linked to the Digital ID. Verified through the Digital ID app, this mailbox facilitates secure, individual communication with users.

A more user-friendly implementation is an integrated mailbox within the Digital ID app, allowing users to send and receive emails, messages and documents exclusively with government entities. This functionality operates similarly to a standard email client but is restricted to government-to-citizen and citizen-to-government communication. This alternative ensures that users can trust the mail's origin, as all messages and attachments are securely managed within the Digital ID app environment, avoiding transport over unsecured internet channels.

Additionally, this mailbox enables government entities to send legally recognized registered emails, provided appropriate legislation is in place. This method is particularly useful for critical communications such as court orders or tax notifications.

A key security feature is the strict limitation of communication to government and citizen interactions. This design protects sensitive government communication and personal information from potential threats, such as the use of public email clients hosted in other countries. By keeping all private information within the Digital ID mailbox, data are securely managed under local legislation, ensuring compliance and safeguarding privacy.

1.3.1.7 DOCUMENT EXCHANGE

Government entities issue various documents to citizens and residents, often in the form of stamped originals for certain cases where a single original is necessary. However, many documents can now be issued digitally. To secure digital documents and link them to the identity of a citizen or resident, these documents can include a VDS embedded in PDF format. The VDS secures key document data with a digital signature (refer to Chapter 2.4 Visible Digital Seal (VDS) Technology). Such secured documents can be sent to users electronically, such as residence visas for residents or civil status extracts for citizens.

Sending personal documents via regular email poses security and privacy risks. A Digital ID application enhances security by supporting the issuance, exchange and presentation of electronic documents. This is particularly relevant in cases where government systems do not fully interconnect due to privacy concerns. For regulated sectors like banking, telecommunications and insurance, which operate separate systems, official documents issued by the Government are essential for users to prove eligibility and legal presence in the country, fulfilling regulatory and Know Your Customer (KYC) requirements. When a government entity issues a digital document to a citizen, the Digital ID app securely stores it in PDF format, linking it to the user's identity and purpose. These stored documents can have attributes and policies, similar to digital passes, including validity and other criteria. If a user needs to provide a specific document from their Digital ID document repository, such as an identity card, passport copy or residence visa, they can consent to share it with a requesting entity. For example, during a bank account application, the Digital ID app enables the user to meet KYC requirements by securely submitting the necessary documents. Biometric authentication provides an additional layer of security for such transactions.

The secure document repository within the Digital ID app is designed to handle all types of documents issued to the user. Like digital passes, these documents are linked to the user's identity and are disclosed only with their explicit consent, ensuring both security and user control.

1.3.1.8 VALIDATED ID TOKEN

Digital ID systems enhance customer identification processes commonly required by regulated industries such as banking, telecommunications and insurance. To comply with anti-money laundering regulations and prevent tax evasion, these businesses must maintain high levels of identity assurance through periodic customer identification and verification. This process, known as Know Your Customer (KYC), typically includes verification against national ID documents, which can be facilitated through digital document exchange as outlined in section 1.3.1.7.

Digital ID systems can implement secure identity tokens with selective disclosure capabilities. The authentication process begins when a service provider sends an authenticated request to the Digital ID managing authority, specifying required personal information. The communication channel requires secure authentication to verify the service provider's authorization. To ensure authenticity, the service provider digitally signs the request token using their private key. This request token includes essential information such as the transaction type, whether for KYC or other purposes.

When the Digital ID service provider receives a request, it forwards it to the citizen's Digital ID application. The application displays the requested information and requesting entity to the user. Citizens can review and authorize the disclosure, with selective disclosure capabilities where applicable, though some transactions may require mandatory information. The system clearly presents both the purpose and the requesting service provider's details. To establish the necessary assurance level, the process requires biometric or PIN authentication before proceeding.

Upon receiving user approval, the Digital ID managing authority generates a unique Digital ID token containing the approved information. This token incorporates both the signed request token and purpose and is then transmitted to the requesting provider. Through request token binding, the system ensures the token can only be used by the original requester, maintaining security throughout the process.

The inclusion of the signed request token significantly enhances security, particularly for long-term KYC information storage. The token contains cryptographically verifiable proof of the original request and supports variable validity periods, ranging from short-term to indefinite archival storage. Importantly, the system enables offline verification through embedded authentic signatures, maintaining both security and user privacy while meeting regulatory requirements for identity verification and record-keeping.

1.3.1.9 TAKEAWAY AND SUMMARY

For the implementation of a Digital ID, various functionalities are available, and key considerations must be addressed:

- **Application ecosystem:** A key requirement is the availability of an application ecosystem, including at least a web application to manage the user's Digital ID and mobile applications. These should support SSO functionality, which is crucial for managing online services.
- **Identity management infrastructure:** A centrally federated SSO system is recommended. This system allows the segregation of portals for different entities while enabling the use of centrally managed Digital IDs for users to log in to various portals.
- **Verifiable credentials:** Digital ID passes for different applications should support both online and offline operations to ensure flexibility for various use cases.
- **Social engineering threats:** As systems become more secure, social engineering by fraudsters has emerged as a major threat. Humans often represent the weakest link in the security chain.
- **Cyber threats and identity theft:** It is essential to counter cyber threats and identity theft through user communication and awareness campaigns. Technical measures, such as controlled communication via a mobile app mailbox, can further enhance security.
- **Digital signature:** Digital signature functionality is a key feature of advanced digital identity systems. It requires higher levels of user education and robust security measures. Legislative support is mandatory and foundational for enabling digital signatures.
- **Inclusion of key users:** The primary users, including government-regulated commercial businesses that require KYC procedures, should be considered during functional planning.

1.4 USE CASES OF DIGITAL IDENTITY

Digital ID and the functionalities offered by digital identity systems can be applied in almost any scenario requiring user identification. While this is not always relevant for private sector applications primarily focused on service delivery in exchange for payment, it can play a significant role in areas where a person's identity is a critical factor for eligibility.

The specific functionalities utilized in each use case depend on the overall features provided by the Digital ID implementation and the unique requirements of the use case.

Service access

Digital services and all categories are offered by service providers primarily differentiated based on identity and eligibility. For instance, some services are exclusive to citizens, such as special retirement benefits, while others are specific to residents, such as the issuance or extension of residency permits. Other services might be offered to all citizens and residents or even other categories like visitors and tourists. In any case, the primary identification is already an indicator of eligibility, but the services providers prefer other attributes to the identity to determine eligibility. Identification of the user is key to determine the eligibility for a service and following service delivery.

Use case categories

Use cases can be categorized into different groups targeting single or multiple user demographics based on individual eligibility. The categories described in the toolkit are supported by examples, though these are not exhaustive, as the range of use cases is much broader and depends on the specific country and geographical context of implementation. Examples are provided to illustrate the categories and offer a basic understanding of the different use case categories and their requirements.

In Part 2 of the toolkit, implementation guidance emphasizes the importance of carefully evaluating and selecting key use cases and categories to focus on the most viable options and achieve quick wins for both the population and the Government.

A digital identity system and Digital ID can generally support all use cases. However, government-issued Digital IDs are typically limited to governmental use cases to mitigate risks. This restriction is primarily driven by the need to address legal challenges associated with connecting private entities to government IT networks and applications.

Main categories of use cases

- **Governmental**

  Services offered directly by governmental entities or ministries.

- **Regulated private sector**

  Services offered by organizations that are private but regulated by the Government.

- **Private sector**

  Any private sector use case that is offered from a privately owned business.

- **Special use cases**

  Are all use cases that are offered by special entities.

Use case functionality matrix

The functionality matrix provides a brief overview of the common functionalities associated with each use case category. It aims to illustrate the basic concept of functionality distribution, though the actual implementation and usage depend on the implementing authority and government regulations, which may differ from the general approach described below. Special use cases are not included in Table 4, as their functionalities are tailored to specific user groups, and the Digital ID system may not be

integrated with the general government-issued Digital ID. The term partial indicates that the functionality may only be used in a limited capacity.

Table 4 reflects the perspective of a government Digital ID implementation. For private sector implementations, which are outside the scope of government-issued Digital IDs, a private Digital ID could be operated by a private trust service provider. Such private sector implementations are beyond the scope of this discussion on government Digital IDs.

Table 4. Functionality – use case matrix

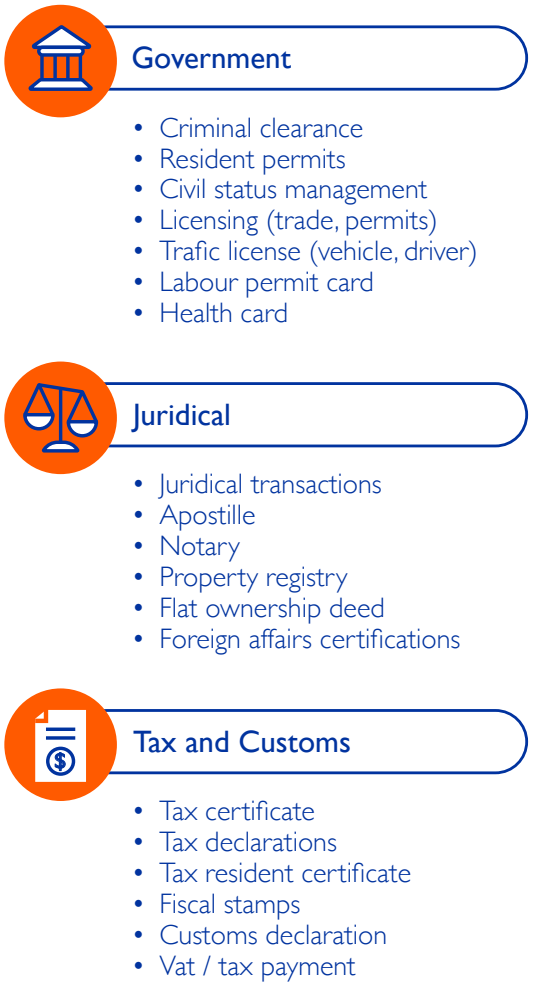
FUNCTIONALITY / USE CASE	GOVERNMENTAL	GOVERNMENT REGULATED	PRIVATE SECTOR	COMMENT
Single Sign On (SSO)	✓	Partial	✗	Largely depends on the nature of the regulated business. In some countries, users are allowed to log in to regulated entities.
Transaction Approval	✓	Partial	✗	Same as SSO, strongly depends on the implementing authority.
Web Portal	✓	N/A	N/A	The Digital ID web portal functionality serves primarily as an administrative tool for users and is accessible only to the Government and the user.
Digital Passes (VCs)	✓	✗	✗	
Digital Signature	✓	✓	✓	
Mailbox	✓	✗	✗	
Document Exchange	✓	Partial	✗	Partial exchange may be limited to receiving documents but not sending them, such as identity proofs or other documents exchanged
Validated ID Token	✓	✓	Partial	Private business could have access, depends on the strategy

1.4.1 GOVERNMENTAL USE CASES

Governmental services are the primary use cases for Digital ID and digital identity systems. These services are provided entirely by government entities or ministries and are targeted at individuals and private businesses (juridical persons). The services are delivered through various government entities via web portals or mobile applications, with SSO functionality serving as the key feature for user login and identification. Additionally, transaction approvals are frequently used to validate submissions and actions.

Some applications may also issue digital verifiable credentials, which can be used offline. Examples include digital health cards, insurance cards, driver's licenses and vehicle licenses. These verifiable credentials are stored in the user's digital wallet within the Digital ID application on their smart device.

Figure 9. Governmental use case examples

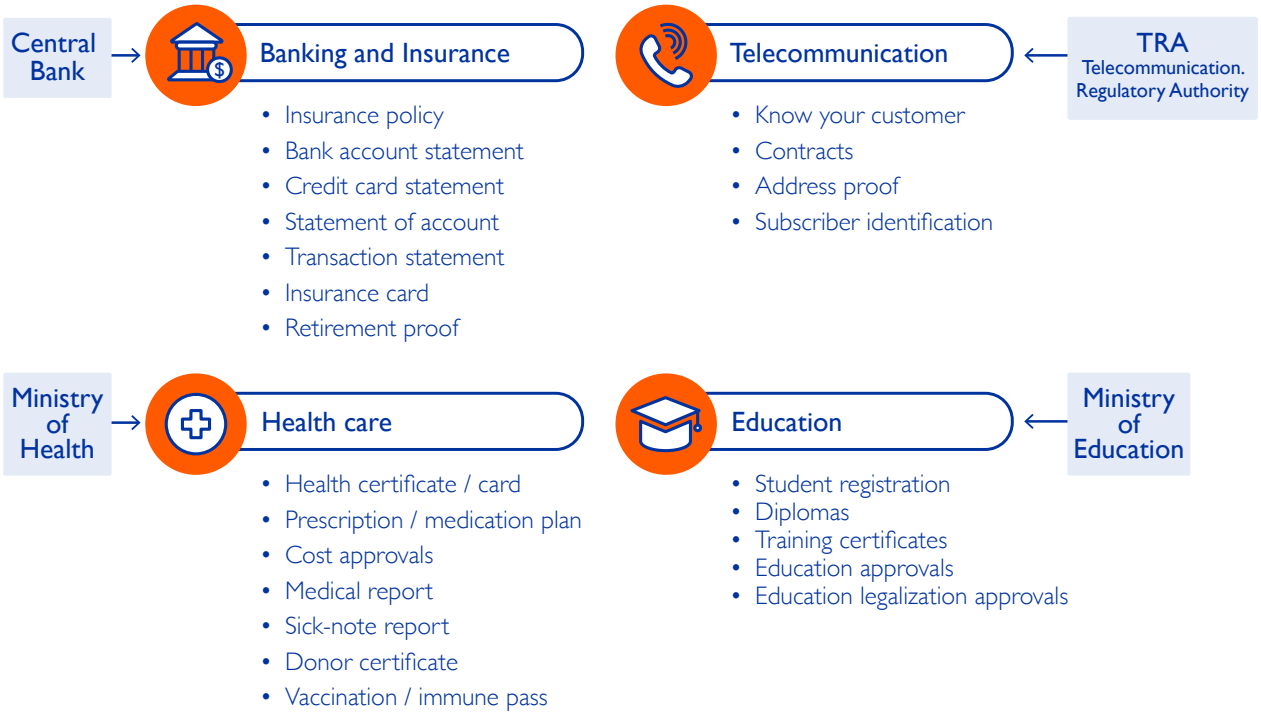


1.4.2 GOVERNMENT-REGULATED PRIVATE SECTOR USE CASES

Government-regulated use cases primarily involve private sector businesses operating in highly regulated markets. For example, regulators such as the central bank for the banking sector and the telecommunication regulatory authority for the communication sector define rules for customer identification. These businesses are required to follow stringent identification procedures to ensure that services are provided to individuals with verified and clear identities.

Due to these regulations, it is more practical to grant such entities access to Digital ID services or, at a minimum, provide methods and systems to automatically verify clients' digital identities with legal validity. Digital ID in regulated sectors can help prevent money laundering and tax evasion, and support efforts to combat fraud and service misuse.

Figure 10. Government-regulated use case examples and regulators



1.4.3 PRIVATE SECTOR USE CASES

Private sector use cases may not directly benefit from all Digital ID functionalities. The direct connection of private entities to a government-managed Digital ID system and infrastructure carries certain risks that most governments aim to avoid.

Utility supply entities might be an exception, as utilities in some countries are fully owned by the Government or operate under a government-controlled monopoly. In such cases, utility supply entities can be considered government entities or government-regulated entities. Similarly, this may apply to other sectors and businesses, particularly government-owned private companies, such as railway companies in certain countries. These companies are structured as private entities, but the Government retains full or majority ownership of their shares.

Determining the policies under which a private sector company can access directly connected Digital ID systems falls under the jurisdiction of the governing authority. The categorization and separation presented in this toolkit are intended to illustrate the varying nature of use cases and their differing levels of participation in the Digital ID ecosystem.

Private sector trust providers

The establishment of private trust providers could offer a solution to allow private entities to participate in Digital ID services, including direct connections for SSO and transaction authorization. The Digital ID systems used by private trust providers are technically similar to those implemented by governments. The key difference lies in the trust framework, which is tied to the private trust provider rather than directly to the Government's Digital ID infrastructure.

Private trust providers operate under a legislative and regulatory framework specifically designed for them within the broader Digital ID legislative framework. Once this legislation is established, private trust service providers can be considered government-regulated entities. They may then have the potential to directly connect to government infrastructures or use government authentication methods to verify user identities.

Under this structure, users must first onboard with the private trust provider by utilizing their government-issued Digital ID and digital credentials. The trust provider derives the user's identity based on the Government-issued Digital ID and can subsequently offer a wide range of trusted services under its own offerings and responsibilities, as defined by the applicable legislation.

In some countries, banks, insurance companies or telecommunication providers already offer such services. These entities often possess highly sophisticated IT infrastructures and operate in strongly regulated sectors with stringent KYC procedures, which are also required for onboarding to a private trust service provider.

Figure 11. Private sector use case examples

1.4.4 SPECIAL DIGITAL ID USE CASES

Special use cases are typically considered outside the scope of a regular government-managed Digital ID system. While Digital ID systems in this sector may follow similar principles and functionalities – partially or fully – they operate under specific legal frameworks and dedicated operations. These use cases primarily serve special user groups that are not included in the legal population enrolled in a population register.

In some instances, the infrastructure may not be operated by the Government. Instead, other international entities, such as United Nations bodies and agencies, may manage the related identities.

Each special Digital ID use case described in this toolkit follows its own logic and may vary significantly from country to country. The description below illustrates one possible approach to implementing such use cases, highlighting the principles, special circumstances and operational requirements involved.

1.4.4.1 COUNTRY VISITORS USE CASE (TOURISTS)

Visitors and tourists entering a country with a travel passport are typically registered in the immigration system, which is connected to the country's border control. Some countries with a high volume of visitors and tourists have started providing Digital IDs to these individuals, based on the identity information collected during border crossing and registration.

These countries collect biometric data such as fingerprints, facial recognition and iris scans to verify each traveller's identity. This process ensures that a traveller can be identified as a new visitor or matched to a previous visit. After verification, an immigration ID is issued to the traveller, under which all entries and exits are recorded. Biometric verification ensures that even if a traveller changes their name or nationality, they can still be identified. In such cases, the traveller is typically referred for second-line border inspection, and once their identity is confirmed, the updated information is linked to the same immigration ID.

This system operates similarly to a population register but is based on travel identity rather than legal identity. Once a traveller is registered with biometric data and the associated system processes, it becomes technically possible to issue a Digital ID. This Digital ID can facilitate access to online services for the traveller, such as obtaining a SIM card, accessing emergency health-care services, linking to insurance information or recording vaccination details, especially during pandemics.

Digital ID could also streamline border control processes, enabling faster and easier entry and exit for known and eligible travellers, even at a large scale.

Nevertheless, the implementation of Digital IDs for visitors as part of service provision remains a special use case.

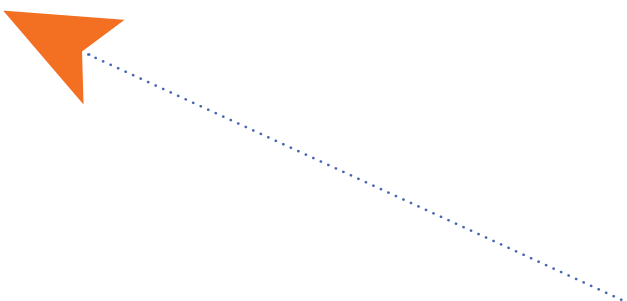
1.4.4.2 MIGRATION SUPPORT AND IDENTITY MANAGEMENT

The identity of migrants, whether moving between countries regularly or irregularly, should be managed by the host country or supported during border crossings, such as in free movement zones. Migrant enrollment is often outside regular immigration databases or population registers but must adhere to the same technical standards and security requirements. The management and responsibility for the infrastructure and the potential issuance of migration documentation lie with the host country. General registration and identification are crucial to providing services to migrants and granting access to certain types of aid or services within the host country.

A significant challenge in registering migrants is verifying their identity using the documentation they provide. Many migrants may lack proper identification, necessitating the issuance of digital identity credentials. Biometric technology plays a critical role in ensuring the uniqueness of identities and in deduplicating migrant databases. Migration-related databases should be connected or synchronized with national systems to prevent duplicate registrations, which can be identified through data synchronization.

IOM supports its Member States in matters related to migration identification. However, IOM does not have the mandate to issue documentation for migrants. The responsibility for issuing documentation remains with the host country.

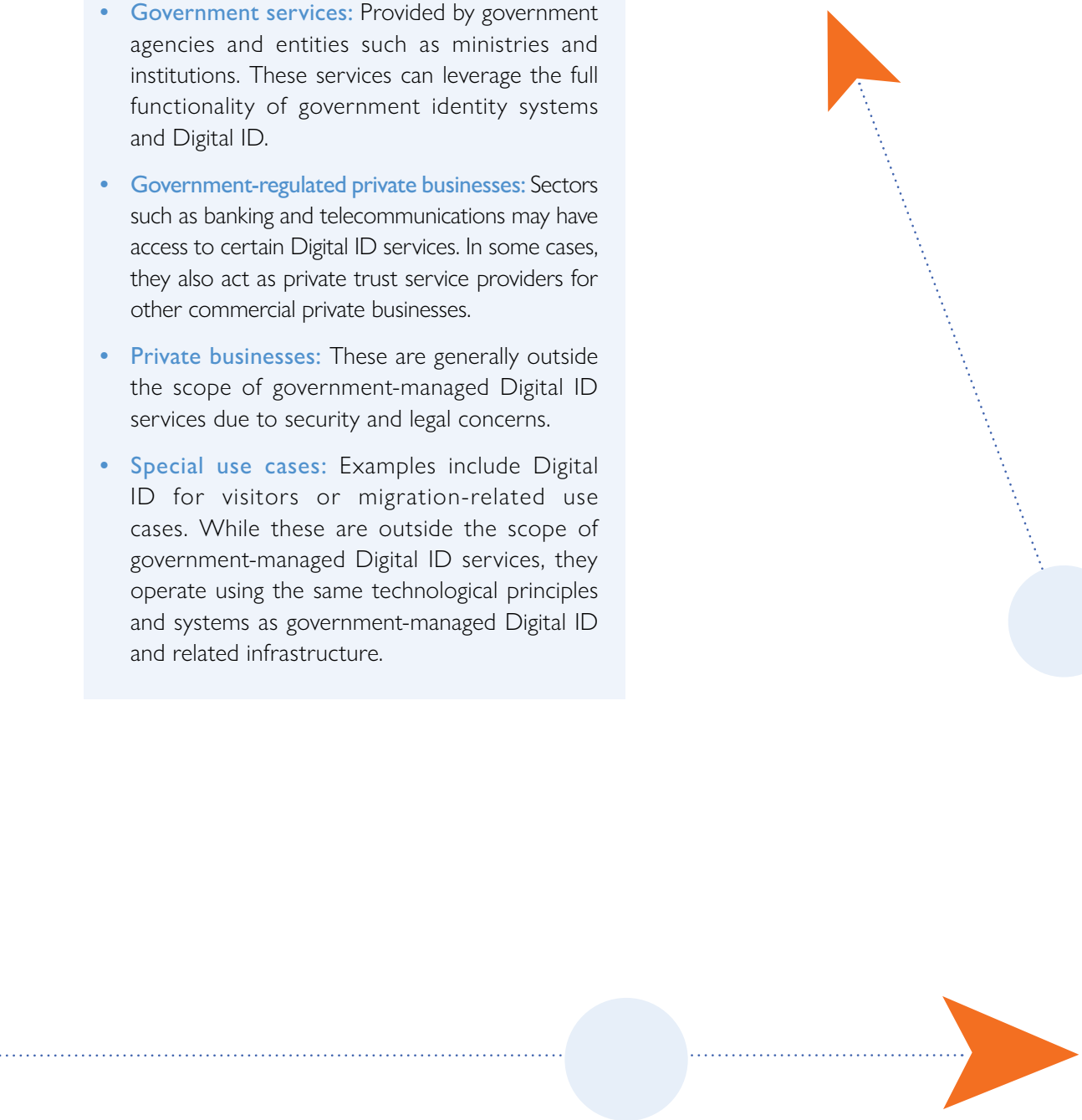
Part 3 of this toolkit describes a use case for Digital ID and digital credentials for migrants crossing borders within a free movement zone established between two or more countries under a bi- or multilateral free movement agreement.



1.4.5 TAKEAWAY AND SUMMARY

Digital ID can be utilized in nearly every sector that offers digital services. These services can be grouped into different categories:

- **Government services:** Provided by government agencies and entities such as ministries and institutions. These services can leverage the full functionality of government identity systems and Digital ID.
- **Government-regulated private businesses:** Sectors such as banking and telecommunications may have access to certain Digital ID services. In some cases, they also act as private trust service providers for other commercial private businesses.
- **Private businesses:** These are generally outside the scope of government-managed Digital ID services due to security and legal concerns.
- **Special use cases:** Examples include Digital ID for visitors or migration-related use cases. While these are outside the scope of government-managed Digital ID services, they operate using the same technological principles and systems as government-managed Digital ID and related infrastructure.

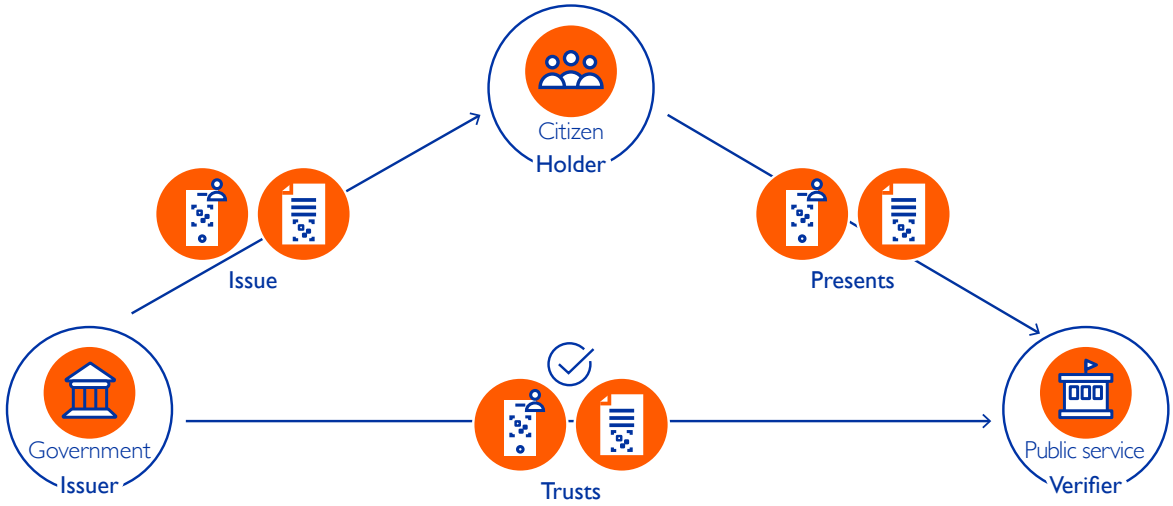


1.5 DIGITAL IDENTITY MANAGEMENT FRAMEWORK

The Digital Identity and Digital ID System involve three main actors, connected through a trusted relationship. Their interactions and information exchanges are secured by a PKI.

The Digital ID described in this toolkit assumes a government-managed system, used directly by government agencies and service providers. The identity provided is based on the legal identity and, if defined by policies and legislation, carries full legal validity.

Figure 12. Digital ID actors



Issuer – Government

The holder of the population registers or main database managing the legal identity of citizens is, at the same time, the issuer of the Digital Identity credential. In the case of a mobile application, it also serves as the issuer of the Digital ID. The issuer is primarily responsible for the identity, security and integrity of the data.

Holder – Citizen

The holder of the digital identity and Digital ID is the citizen who has enrolled in the identity database and to whom the issuer provides the digital identity credential and Digital ID. The digital identity credential can also be linked to an identity document in various formats, such as one with a chip and/or VDS. A key characteristic is the digital credential, which includes a secure proof of integrity and origin through the issuer's digital signature.

Verifier – Public service entity

In the framework presented, the verifier is another public service provider. The citizen presents their digital identity or Digital ID to the service provider, which verifies the identity using the credentials issued by the issuer. The verifier trusts the issuer and, after successful verification, accepts the presented identity.

General threats in the framework

The general responsibility for verification security lies with the verifier. They must ensure the correct issuer credentials are used to sign the citizen's identity. This security is managed through a PKI trust model. The same principle applies to verification tools, which must be approved by the verifier. In the presented use case, these tools are provided by the issuer and are trusted.

A significant threat to digital identity is the use of malicious or manipulated verification tools, which could approve a false identity and display it as valid. Security and trust are essential on both ends – issuance and verification. For this reason, and due to the potentially linked liability, most governments are cautious about directly connecting private businesses to government identity systems. Allowing such connections would mean the Government relinquishes control over verification, as the private verifier is responsible for their own operations.

Offline and online verification

The direct online connection of an entity to a government Digital ID system refers to a relationship where the connected entity can utilize the full features of the Digital ID installed on the holder's mobile device. The use of this digital functionality, as described in the toolkit, requires the verifier to be identified by the Government's Digital ID system and authorized and audited for logins and transaction approvals. Such an online connection is not only a security concern but also raises privacy and data protection issues, especially when private businesses are connected.

Offline verification, also known as passive authentication, involves verifying the identity presented in a digital credential (such as a VDS or digital data) without an online connection. This method is accessible to any private business or individual. During offline verification, the integrity and origin of the identity are confirmed by verifying the digital signature. The verifier is responsible for obtaining the issuer's credentials in a trusted manner. Once the digital identity credential or data is confirmed to be valid, the verifier must ensure that the person presenting it is the rightful holder of the identity.

Offline or passive authentication provides significantly better security compared to a simple visual inspection of an identity document. Depending on the verification policy a verifier follows for their business, they must ensure their measures are robust enough to hold up in court in case of disputes or doubts over the identity and related commercial transactions.

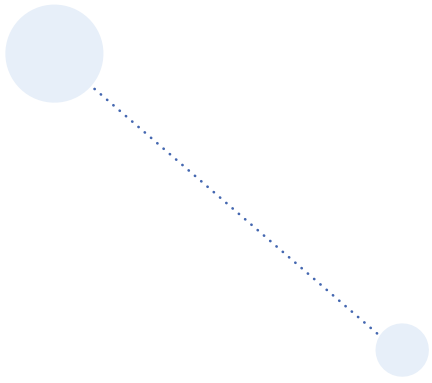
For most businesses, offline verification is sufficient. The digital credential, such as a VDS, often offers higher identity security than a standard visually presented ID document.

Other risks

Offline verification is partially effective for online businesses, though commercial service providers or merchants often prefer using a digital identity. Another challenge arises with service providers operating across multiple countries and borders. Cross-border activities introduce complexities, as the use of a legal identity across borders is only possible if two countries bilaterally agree to it or if the countries belong to a Free Movement Zone[12] with a harmonized legislative framework, such as the European Union.

A common alternative is the use of travel documents as identity documents, which introduces additional risks. Travel documents are designed specifically for travel and border verification purposes. While private entities can verify travel documents, they are not fully qualified to do so, and the associated legal responsibilities carry significant risks. For example, individuals may change their names in travel documents, hold multiple nationalities or possess multiple passports. As a result, the true legal identity of an individual cannot always be assumed.

This issue is particularly problematic in scenarios involving international financial transactions that require measures against tax evasion and anti-money laundering. In such cases, individuals may have an incentive to conceal their true identity and present false credentials, exploiting the limited verification capabilities of the private sector with respect to travel documents.



12 Stephan D. Hofstetter, Rajeshkumar Raja, *Free movement zones: guide for issuance and border management* (Geneva, IOM, 2021).

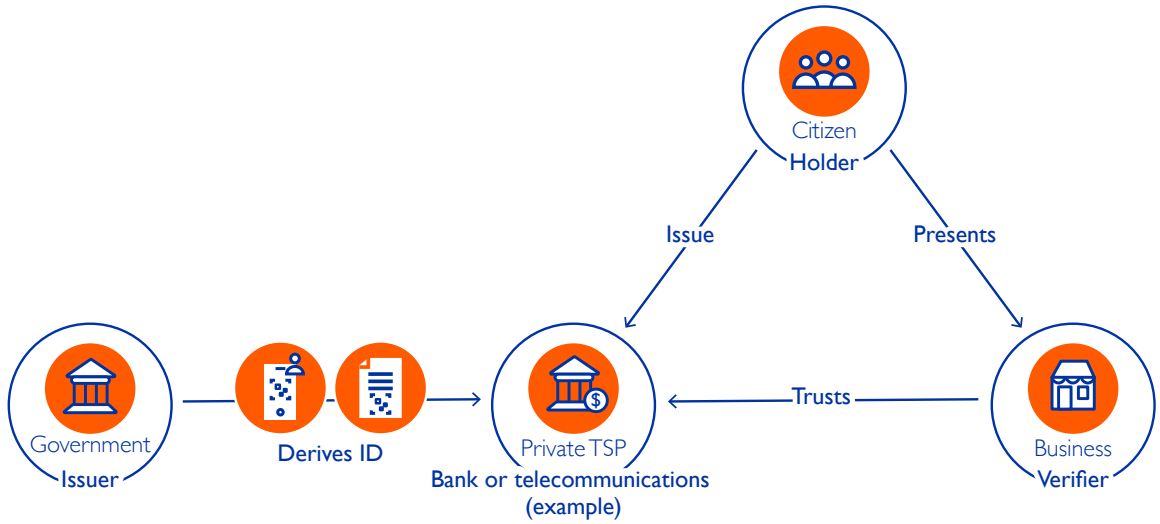
1.5.1 PRIVATE TRUST SERVICE PROVIDER MODEL

For providing Digital IDs to private businesses, the Private Trust Service Provider (TSP) model is a viable option. This model is based on an identity broker that acts as an intermediary between the Government and other actors within the Digital ID Framework. The holder requests a Digital Identity based on the identity database managed by the private TSP.

The private TSP can be a government-regulated service provider that derives identity information from the Government to maintain its own identity database. The derived information would be limited and must have the user's consent. The TSP model requires legislative regulation to ensure that the TSP adheres to local data protection and security regulations for handling personal data.

The TSP could be any authorized company, such as a bank or telecommunications company, as these entities are already regulated by the Government and operate under strong KYC policies. The provision and regulation of TSPs are the responsibility of the country and its related legislative framework.

Figure 13. Trust Service Provider (8TSP) model



Cross-border commercial use of Digital ID

The private TSP model does not necessarily address the cross-border activities required by businesses. In many cases, the real identity of a consumer is not relevant, as commercial transactions are typically accompanied by payment transactions. Identifying the consumer using their legal identity is often not legally required, except in regulated industries such as banking, telecommunications, or other sectors that mandate legal verification in accordance with local KYC rules.

Many commercial entities in such cases rely on third-party identity providers, which identify individuals only by their email addresses or mobile numbers. Examples of such providers include Apple ID, Microsoft Authenticator and others. These providers create digital identity credentials based on their own vetting processes and information, which they offer to merchants, sometimes linked with payment collection. These providers operate under their own private frameworks, using Digital ID systems without government regulation. Their business model is based on the fact that merchants are primarily interested in receiving payment for their goods and services. These services are often provided across borders and are not bound to full legal validity.

In the event of a dispute, a commercial business must defend its case in court. To avoid such legal battles, businesses often price a certain level of risk into their products or services to cover potential losses due to identity issues. Some providers, such as PayPal, offer merchants and consumers insurance or revocation rights for transactions.

Private transactions and merchant activities are outside the scope of this toolkit. This section is intended only to illustrate that the same technology and technical framework is widely used in commercial settings.

1.5.2 DIGITAL ID ECOSYSTEM

The Digital Ecosystem is built on five key pillars, all of which are integral to the implementation of a Digital Identity.

Figure 14. Digital ID ecosystem

1.5.2.1 GOVERNANCE

The governance of digital identity should be closely aligned with the governance of general identity management within the country. It should be assigned to an existing ministry or agency that already manages identity at the federal level. If no such agency exists, a separate autonomous agency for national identity could be established at the federal level to centralize responsibility for identity management within a single entity. This entity would be responsible for managing the population identity database, capturing biometric information and issuing digital identities. In many cases, such organizations are directly linked to the entity responsible for issuing identity cards.

To implement a uniform system across the country, the entity managing identities and digital identity should operate at the federal level and be endorsed by the country's governing authority or a high-level decree. The governing agency would be responsible for supporting the required legal framework, establishing and managing the necessary systems and business processes, and ensuring robust security and privacy measures. Additionally, the agency should set up essential organizational units such as finance, compliance, operations and security, to effectively manage the operation of digital identity systems.

Related actions are:

- Establishment of the governance framework;
- Identification and endorsement of an existing or new federal entity to manage Digital ID;
- Definition of the scope and mandate of the identity managing entity or organization;
- Establishment of operational units for Digital ID;
- Staffing and financing of the governance structure and projects.

1.5.2.2 LAW AND POLICY

The legal framework is essential for the implementation of Digital ID systems and the provision of digital services. Laws and regulations should enable electronic identification using Digital ID and endorse the related technical methods. Additionally, the legal framework must establish provisions for privacy protection, inclusion and non-discrimination in the digital space when using Digital ID or related digital services.

Special attention should be given to legislation on digital signatures. In many countries, the legal validity of a signature is defined only for handwritten signatures. To facilitate the transition from paper-based to digital services, legislation must equate digital signatures with handwritten ones as an alternative method. This equalization avoids the need to amend other laws tied to handwritten signatures and supports the move to fully digital processes.

Digital signatures are a critical element for completing the digital service cycle in government operations. They enable citizens or businesses to return digital documents, applications and reports in digital format, eliminating the need to send scanned paper documents. For an electronically organized government, achieving a fully digital service cycle should be the ultimate goal.

The laws and policies required for Digital ID systems depend on the country's existing identity management laws. These laws must be reviewed to ensure they support electronic authentication and identification. To bolster Digital ID systems, a separate law or bylaws may be issued to incorporate Digital ID into the general identity infrastructure. This could involve extending existing digital electronic ID (eID) laws or enacting new laws specific to Digital ID. Regulating the provision of trust services within Digital ID legislation is also advisable.

Special consideration should be given to regulations governing KYC policies in government-regulated sectors. Banking, telecommunications and insurance companies are typically bound by strict KYC requirements to ensure international compliance with anti-corruption and sanctions rules. Digital ID can significantly enhance the security of KYC procedures, but the relevant legislation must explicitly allow its use.

In many cases, KYC regulations lag behind general government policy. Addressing these regulations early in the process is recommended, as they enable key use cases involving large numbers of citizens and businesses.

The European Union provides an example of a comprehensive framework through its eIDAS regulation, which formalized legislation for digital trust services and signatures. This regulation was enhanced with eIDAS 2.0 to ensure universal access for citizens and businesses to secure and trustworthy electronic identification and authentication using Digital ID and digital wallets.

Key considerations for the legislative framework are:

- Ensure that existing laws allow the usage of Digital ID in government services;
- Implement new laws to regulate the use of Digital ID;
- Pass legislation on data privacy and protection;
- Ensure digital signature regulations and related security frameworks align with the equalization of digital signatures and handwritten signatures;
- Regulate digital trust services and identity services;
- Review KYC policies of government-regulated businesses to allow the use of Digital ID.

1.5.2.3 PROCESS

Digital ID systems and general identity systems are considered critical infrastructure, as they form the foundation for many other electronic government services. It is essential that Digital ID services remain consistently available and capable of meeting demand. As more government infrastructure becomes digitalized, it will increasingly rely on Digital ID services to function effectively.

Any interruption or compromise in security and privacy could have a severe impact on the entire government service structure. Therefore, the implementation of robust operational processes is crucial, requiring close monitoring and control to mitigate operational risks and prevent interruptions.

Key considerations for the processes are:

- Compliance with regulatory requirements;
- Operational risk management process;
- Operation policies and procedures;
- Business continuity processes to ensure service availability for the infrastructure;
- Service quality and continuous improvement processes;

- Development and testing procedures for new features and software quality management;
- IT service management and change management processes;
- Customer awareness and education processes;
- Partner policies and connection management to integrate with other government electronic services;
- IT Security and data protection management processes.

1.5.2.4 TRUST AND PRIVACY

Trust and privacy are key pillars of digital services and Digital ID systems. Digital ID and identity management, in general, handle citizens' personal data and related transactions with metadata. Any compromise in trust or privacy can significantly impact the services and overall governance of a Digital ID implementation.

The management of trust and privacy involves multiple dimensions and considerations:

- **Integrity of citizen data**

  Digital ID systems access citizen data, and the digital credentials contain this sensitive information. The system must always protect and ensure the integrity and validity of the data.

- **Trust in credentials and verification tools**

  Credential verification requires trusted tools that users can rely on. Verifying credentials with non-trusted applications can lead to fraudulent scenarios, where manipulated identities appear valid because the tool itself has been compromised by a fraudster.

  To ensure trustworthiness, governments should provide and maintain official tools for Digital ID credential verification or certify third-party tools through a robust certification process. Only tools that users and verifying parties trust will ensure the necessary level of confidence in the system.

- **Data privacy**

  The Digital ID system must implement measures to guarantee data privacy in compliance with local privacy laws and regulations. Non-compliance can severely undermine user trust in the system and the operating organization.

  Data privacy measures should protect against cyberattacks and unauthorized disclosures and prevent the misuse of private data. These measures must be both technical – covering storage and communication interfaces – and organizational, such as policies and compliance reviews.

  The system should also ensure that citizen data are collected, stored and used only with the individual's consent and solely for the intended purposes.

- **Trust framework**

  The trust framework supporting the Digital ID system and digital signature functionality must be managed with the highest levels of security. The integrity of the PKI, which underpins the system, is critical to maintaining trust in the issued digital credentials and Digital ID.

  Security relies on the confidentiality of secret keys managed by the system's administrators, the protection of the Digital ID wallet application, and the integrity of all related credentials. A compromise in the PKI would have a severe impact on the application and functionality of the Digital ID system.

  Additionally, the trust framework should include organizational security measures and regular audits to reinforce user trust in the system.

- **Privacy and trust by design**

  The system's design and implementation must adhere to the principles of "privacy and trust by design." The architecture should treat trust and privacy as central elements, ensuring these values are embedded throughout the infrastructure.

1.5.2.5 TECHNOLOGY

The technology used and implemented for Digital ID must be innovative to achieve high levels of functionality, flexibility and reliability while being thoroughly tested. For implementation, the total cost of ownership should be balanced against the benefits for specific use cases. Sometimes, simple yet innovative technology can be more effective than sophisticated implementations.

- **Physical credentials**

  Physical credentials are not directly part of the Digital ID implementation, but their choice can influence and support it. If the chosen technology permits, physical credentials can facilitate the onboarding process for Digital ID. For instance, during onboarding, a physical credential could be verified to ensure that only the credential holder can enroll their mobile device.

  Digital ID applications requiring higher levels of security might also use physical credentials as an additional measure. For example, presenting a physical credential to a digital application can confirm that a transaction is being conducted by the rightful credential holder. The chosen technology should be cost-effective and complement Digital ID technology rather than compete with it.

- **Biometric identification**

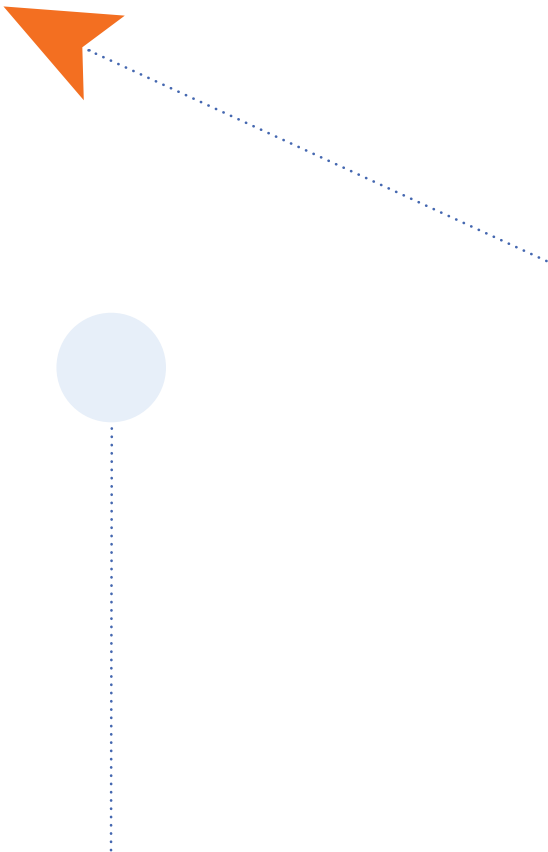
  Biometric technology enables Digital ID applications to verify whether the current user is the rightful owner of the Digital ID. A critical factor in biometric systems for Digital ID is the ability to detect "liveness," ensuring the person presenting the biometric is alive and not using a photo or other spoofing method.

  Biometric technology on mobile devices typically relies on facial recognition, though fingerprint technology is advancing for mobile use. Key considerations for implementing biometric systems include: the type of biometric technology used, user handling and convenience, accuracy of the system, liveness detection capabilities and use of template-based systems with secure template storage in digital credentials.

- **Applications**

  The application technology for Digital ID systems is crucial for ensuring device compatibility and scalability. The design of the applications and chosen technology should allow for easy maintenance and scalability to meet transaction demands. The application ecosystem of Digital ID systems comprises several elements:

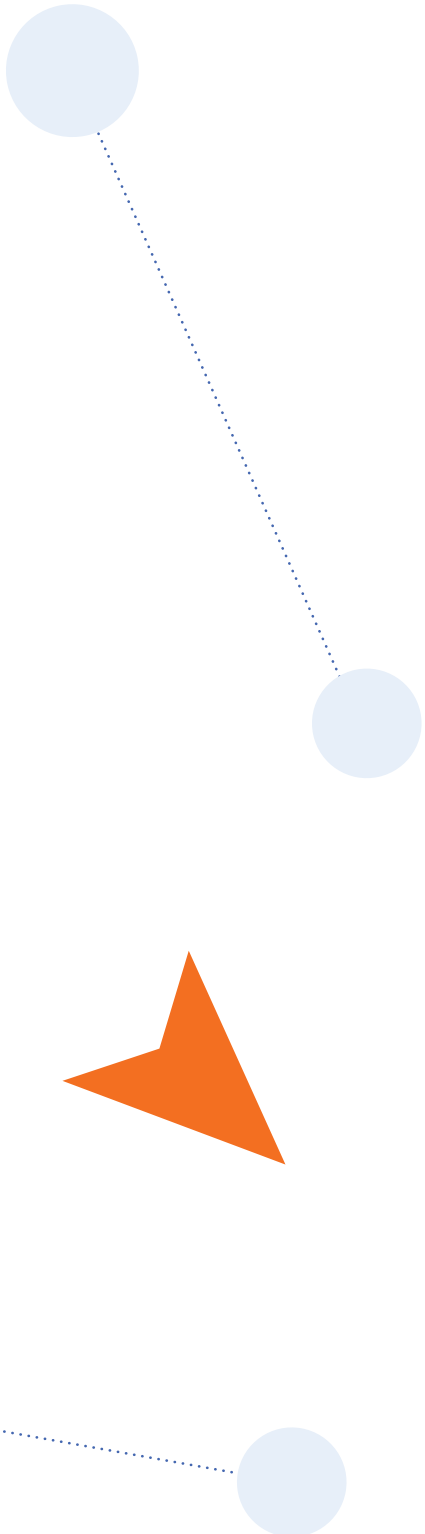
  - Security software and cryptographic hardware components (PKI);
  - Web front-end application which requires web browser compatibility;
  - Back-end applications to manage the server and database communication;
  - Database application to manage the user data and transactions;
  - Offline and online capabilities for the use of credentials and Digital ID.



1.5.2.6 TAKEAWAY AND SUMMARY

The digital ecosystem comprises multiple components, each requiring careful consideration. Key aspects include:

- The implementation of a Digital ID system should address every element of the ecosystem and follow a controlled approach that includes governance, law and policy, processes, trust and privacy, and technology.
- Governance and legislation form the foundation of Digital ID systems, enabling various use cases. Both should be user-centric and aligned with citizens' requirements while ensuring cost savings and administrative benefits for the Government.
- Trust and privacy must be always guaranteed to maintain citizen confidence in and acceptance of Digital ID systems.
- The chosen biometric technology should be carefully selected. Key features include reliable biometric user verification and robust liveness detection capabilities.
- Technology and software should be easy to maintain, offer an optimized cost-benefit ratio, and allow flexible scalability to meet the evolving demands of Digital ID usage.
- Digital ID systems and digital identity infrastructure are considered critical and require high levels of support, trust and confidence from users and government entities alike.
- Strong operational processes, coupled with user awareness initiatives, are crucial for the successful implementation and adoption of Digital ID systems.



1.6 DIGITAL ID KEY CONCEPTS AND TECHNOLOGY

This chapter provides an explanation of the key concepts and technologies used in the implementation of a Digital ID. It serves as a conceptual compendium to explain the background of the technology behind Digital ID. However, it is not intended to be a technical reference for developers.

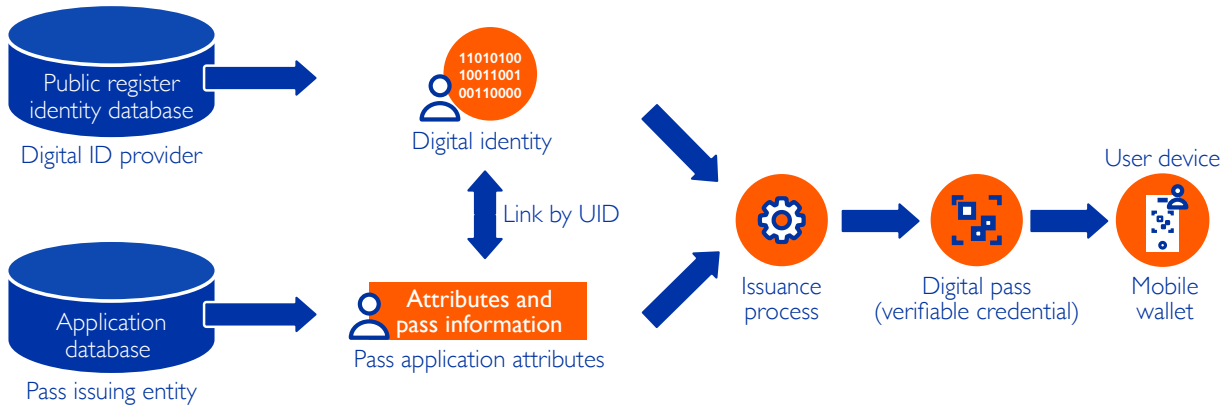
1.6.1 WALLET AND DIGITAL ID PASSES

The digital wallet is a feature of the Digital ID mobile application that allows the app to store offline Digital ID credentials, which can be used in both online and offline transactions. These credentials are often referred to as digital passes.

During the pass issuance process, the user's identity is combined with attributes specific to the pass. These attributes may include additional information provided by the issuing authority (such as for a health pass) or specific parameters such as individual validity or eligibility requirements.

Both the user's identity (linked to their UID) and the pass attributes are digitally signed by the Digital ID issuing entity. Passes are created at the user's request, integrating their identity with the additional information and attributes specified by the issuing authority.

Figure 15. Issuance of digital wallet passes



The technical issuance process is managed by the Digital ID authority, which oversees the wallet and mobile Digital ID application. While the eligibility and additional data for passes are defined by the issuing authority, the process often operates within a shared trust framework. However, it is also possible for passes to use a separate trust framework for signing their digital credentials (VCs). This capability allows the issuance and storage of passes from various trust frameworks within the same wallet.

Mobile wallet pass validity

The validity of a pass is stored within the pass itself, providing significant flexibility. Once a pass expires, it must be electronically reissued, allowing the issuing authority to revalidate the user's eligibility. Doing so ensures the pass cannot be used if the user no longer meets the criteria for its use. For example, a vehicle license pass requires revalidation during each reissuance to confirm that the user still owns the vehicle.

The validity period of a pass varies depending on its application and the governing policy. It may be a one-time-use pass, a short-duration pass valid for seconds or minutes, or a long-term pass valid for weeks or years. In some cases, the issuing policy may mandate biometric verification. For such passes, the user undergoes biometric verification before issuance and the pass is only issued upon successful identity confirmation. This is particularly important for transactions requiring higher levels of user verification or a liveness check, such as pension passes, where revalidation ensures that the pensioner is still alive.

1.6.1.1 DIGITAL ID PASSES (VCS/VDS) ISSUANCE MODELS

Digital pass issuance can be managed in a centralized model, where the issuing authority accesses other entities' databases to issue passes on their behalf, or in a decentralized model, where each entity issues its own passes for the Digital ID wallet. A hybrid model can also be implemented, combining both approaches depending on the government's infrastructure and organizational setup.

For example, in the case of issuing a legal identity pass or a national Digital ID pass, the issuing authority is typically the central authority. If the Digital ID is managed by another entity, the authority hosting the population register or civil registry is usually responsible for issuance.

A key prerequisite for implementing any model to issue Digital ID passes is a unique binding identifier for every individual, linking the Digital ID managing entity with the issuing entity. As explained earlier in this toolkit, it is recommended that the public register operates with a national ID number or another unique numeric identifier. In some cases, existing identifiers such as individual tax numbers or unique social security numbers – though named differently – serve the same purpose: providing a unique identifier for each person. All databases linked to or issuing passes based on the Digital ID must rely on the same unique identifiers to ensure a clear connection to the individual's records. Even in decentralized models, where databases are operated separately for security and privacy reasons, the Digital ID can securely link a pass to an identity only by using a common unique identifier. The presence of such an identifier is a fundamental requirement for Digital ID implementation and reflects a country's digital infrastructure maturity.

The wallet of the Digital ID application can only host passes that are approved and part of the trust framework of the Digital ID managing entity. Due to this security constraint, official passes cannot be loaded into generic wallets provided by mobile phone manufacturers such as Google or Apple wallets, unless the Digital ID managing entity establishes a formal agreement with the mobile phone provider. However, such agreements are unlikely in many countries due to the cross-border legal complexities and the dependency on the provider's governing legislation.

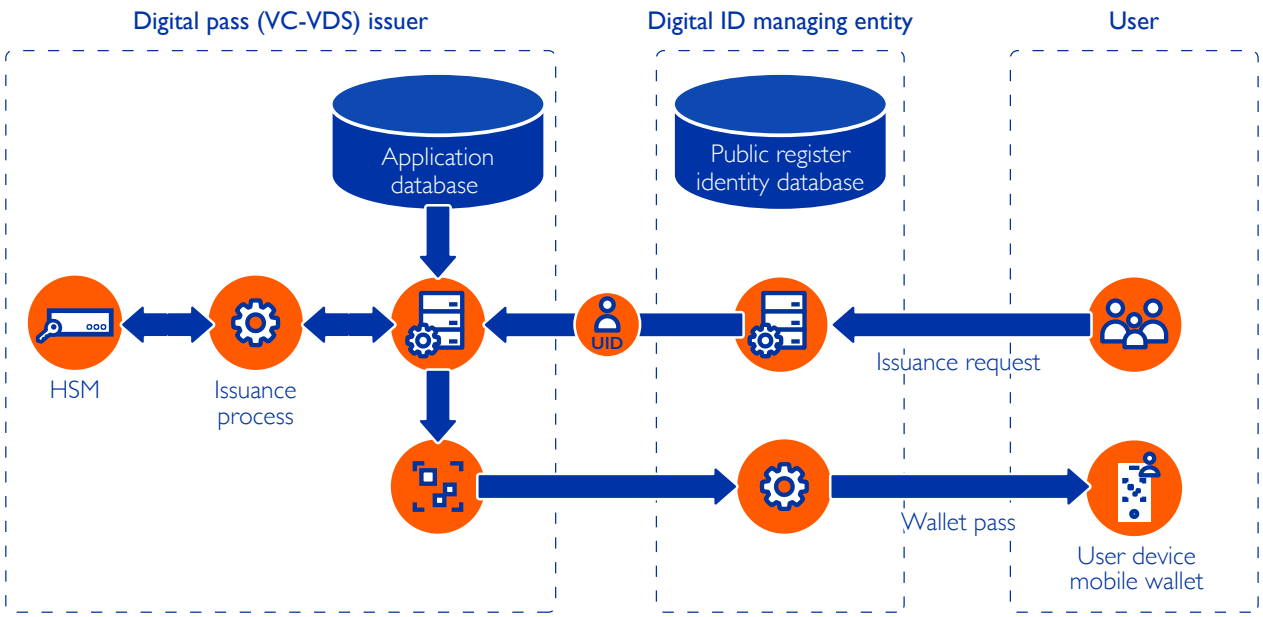
The choice of technical model for pass issuance depends on the digitalization strategy and infrastructure a country wishes to implement or can achieve based on its existing capabilities. The exact model (centralized, decentralized or hybrid) should be defined in the implementation road map, which is discussed in Part II of this toolkit.

Decentralized pass issuance model

In the decentralized model, the entity that wants to issue the digital pass or verifiable credentials, such as VDS, must operate its own trust framework and issuance application on its server. The type of pass is configured with the Digital ID managing entity so that the pass issuance process can be integrated into the Digital ID mobile application.

The user initiates the pass issuance through the Digital ID application, and the Digital ID managing entity redirects the request to the issuer. The issuing entity verifies the user's eligibility by checking the unique identifier to confirm the user's existence and eligibility for the pass. If the user is eligible, the parameters and attributes are retrieved from the database, and the pass is issued. The finalized pass is then sent to the Digital ID managing entity for approval and added to the Digital ID wallet.

Figure 16. Decentralized Digital Pass (VC-VDS) issuance model

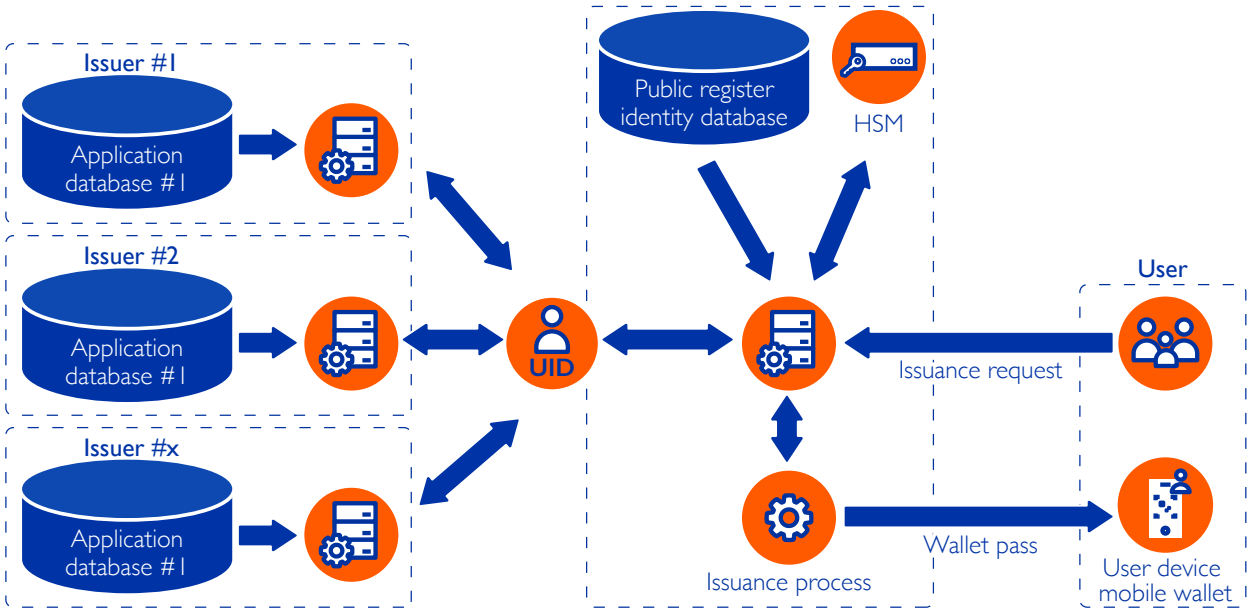


Centralized pass issuance model

In the centralized issuance model, the Digital ID managing entity is responsible for issuing all passes on behalf of other entities, based on the data provided by the pass-owning entity. To facilitate centralized issuance, the Digital ID managing entity requires a database connection to all entities that issue passes. Upon the user's request, the Digital ID managing entity processes the request, retrieves the relevant data and eligibility information from the pass-owning entity's system and database, and issues the digital pass on their behalf within the trust framework of the Digital ID managing entity.

It is also possible for the Digital ID managing entity to operate separate trust frameworks or signer certificates for each individual pass-owning entity. The main complexity in this approach lies in managing the PKI and the associated cryptographic keys required for the various trust frameworks in operation.

Figure 17. Centralized Digital Pass (VC-VDS) issuance

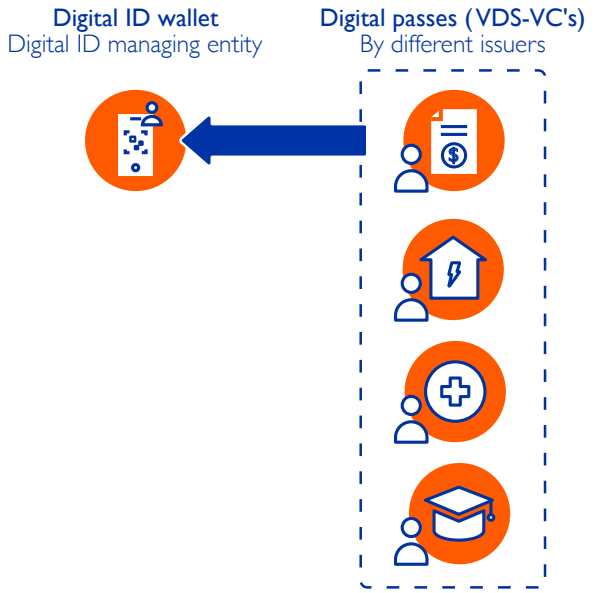


Multifunctionality of a Digital ID

A Digital ID wallet can store multiple passes for various applications, functioning similarly to multifunctional smartcards but in a fully digital format.

Previously, national ID cards were often equipped with smart chips capable of managing multiple applications on a single chip. This approach remains a secure option in certain cases, particularly for storing national identity or legal identity credentials. However, managing multifunctional smartcards involves complexities, such as loading application data at the issuer's office or via a web application using specific security keys provided by the issuer. This process also requires a smart card reader on the user's end, which poses a significant obstacle.

Figure 18. Wallet passes (multifunctionality)



In contrast, a Digital ID wallet offers greater flexibility by securely hosting various passes that can be used offline, like a smartcard, while also enabling online issuance, updates and revalidation of eligibility. Passes in a Digital ID wallet can adapt to dynamic or changing policies managed from a central secure system. This makes the multifunctional Digital ID more cost-effective to deploy and operate compared to traditional multifunctional smartcards, while offering enhanced flexibility and ease of use.

1.6.2 FEDERATION CONCEPTS OF IDENTITY MANAGEMENT SYSTEMS

Identity and SSO on the internet are typically managed through two primary approaches: central identity management and federated identity management. In central identity management, all services are accessed through a single portal that handles login and identity verification for all applications within a unified service window. In contrast, federated identity management involves multiple providers managing identities. Services can connect to an identity provider of their choice, as defined by the application, selecting providers based on trust level, functionality or compatibility. Standard web protocols ensure interoperability and compatibility across different identity providers.

For citizen Digital ID systems, a hybrid model known as "central federated" identity management is often preferred. This approach combines the advantages of both central and federated systems. In this model, identity is centrally managed by a single government entity responsible for the Digital ID platform. This centrally managed Digital ID can be used by various government services through integration with the central identity management system. While the identity is federated from a central source with a single authoritative identity point, its use is typically restricted to government services for liability reasons. In some cases, access is granted to regulated entities such as banks, telecommunications and insurance companies, under strict regulatory frameworks.

In centrally federated identity management systems, the use of Digital IDs in the private sector is facilitated through authorized service providers called Trust Service Providers (TSPs). Government-regulated sectors like banking, telecommunications and insurance can derive Digital IDs from the central government system and provide segregated Digital IDs for commercial use. These derived identities are used by other companies or organizations under the secure frameworks of their regulatory policies. This approach leverages existing KYC frameworks within these sectors, ensuring secure and compliant identity management for private sector applications.

Commercial entities usually verify identities by requesting different forms of information such as address proof, utility bills and copies of ID or passports, to evaluate the individual's identity. Depending on the algorithms and the documents presented, the assurance level of the vetted identity increases. The advantage of TSPs connected to the Government's Digital ID system is the higher assurance of identity, as the Digital ID issued by the Government serves as the root source.

A provider that wants to use the SSO functionality of the Digital ID system must establish a secure connection to the SSO gateway of the identity provider. Only known and trusted service providers should use the SSO service to prevent misuse and fraud, with all usage centrally logged and controlled. A secure connection requires encrypted communication between the SSO gateway and the service provider's server, as well as secure authentication of the service provider. To authenticate, the Digital ID provider must approve the service provider and issue a digital authentication certificate that securely identifies the provider. During the establishment of the secure connection, the service provider uses this digital authentication certificate to authenticate. Once authenticated, the secure and trusted connection is established.

1.6.2.1 PUSH AND PULL CONCEPT

For the SSO functionality, two different concepts are commonly used by Digital ID SSO applications: the pull concept and the push concept.

Pull concept

When a user requests to log in to a portal, the Digital ID system must establish a connection between the SSO gateway managing the identity and the application the user wants to access. In the pull concept, the login portal displays a session code on the screen as a QR code. Simultaneously, the application sends a request to the SSO gateway to log in using this QR code.

The user scans the QR code with the Digital ID SSO application, which then connects to the SSO gateway and requests the login using the QR code. The SSO gateway matches the QR code and establishes the connection. Once the connection is established, the user is prompted to authenticate on their mobile device. After successful authentication, the SSO gateway provides the user information in a secure login to the application the user is attempting to access.

Push concept

The push concept can be used for SSO logins or transaction approvals involving the Digital ID. For SSO login transactions, the user identifies themselves on a website using a unique identifier, such as an email address, mobile number or UID. The application sends a request to the SSO Digital ID gateway to authenticate the user. The gateway, which knows the user's identity and the mobile device they onboarded, sends a push notification to the user's device.

The user opens the Digital ID app by interacting with the push notification and authenticates using the required method. Once authentication is successful, the system grants access to the requested application.

The same push concept is also used for approving transactions when an application requests the user to approve a specific action.

1.6.3 TWO-FACTOR AUTHENTICATION

The term "Two-Factor Authentication" (2FA) describes the process where a user authenticates their identity through two different technologies. Using two or more distinct methods for a single authentication or approval transaction significantly increases security. A potential fraudster would need access to all authentication channels, which is typically not the case.

An example of 2FA is authentication using a confirmation code sent via email or SMS or through a Digital ID app. For instance, if a user logs in with a username and password, the system sends a one-time code via email or SMS that the user must enter to complete the login process. The password alone is insufficient, and if the user forgets or loses the password, they could retrieve a new one using email. In such cases, the system may use another factor, such as an SMS, for additional confirmation. The key requirement is that the primary authentication method must differ from the second factor.

Authentication with a Digital ID app is also considered a second authentication factor. This method is used not only by government Digital ID systems but also in the commercial sector with tools such as Apple ID, Google Authenticator and Microsoft Authenticator. While commercial authenticators work only with vetted identities, their principle of use as a 2FA mechanism is similar to that of government Digital ID systems.

Using a Digital ID app as a second factor provides a high level of security and convenience for users, as it eliminates the need to access emails or search for SMS messages – an issue that can arise, for example, when travelling internationally.

When Digital ID apps are used as 2FA for transaction approvals or generic authentication, the user typically receives a push notification and only needs to confirm with a button or respond to a specific challenge, such as entering a number. Additionally, biometric authentication on the user's phone further enhances the authentication level.

1.6.4 PUBLIC KEY INFRASTRUCTURE (PKI) TRUST MODEL

The Digital ID Framework is built on a (PKI Trust Model to ensure the authenticity and origin of identity and data. Within this trust model, different trust frameworks can be operated and linked as needed. The key principle of PKI is built on a cryptographic methodology where a public and private key pair is generated. The private key is always stored securely, either in a hardware-protected electronic module or in a secure physical location, such as printed on paper and stored safely. The public key, as the name suggests, is "public" and is part of a certificate that can be exchanged.

An entity possessing a private key is called a Certificate Authority (CA), and policies define the purpose of each key. The highest authority in the trust hierarchy is called the Root Certificate Authority.

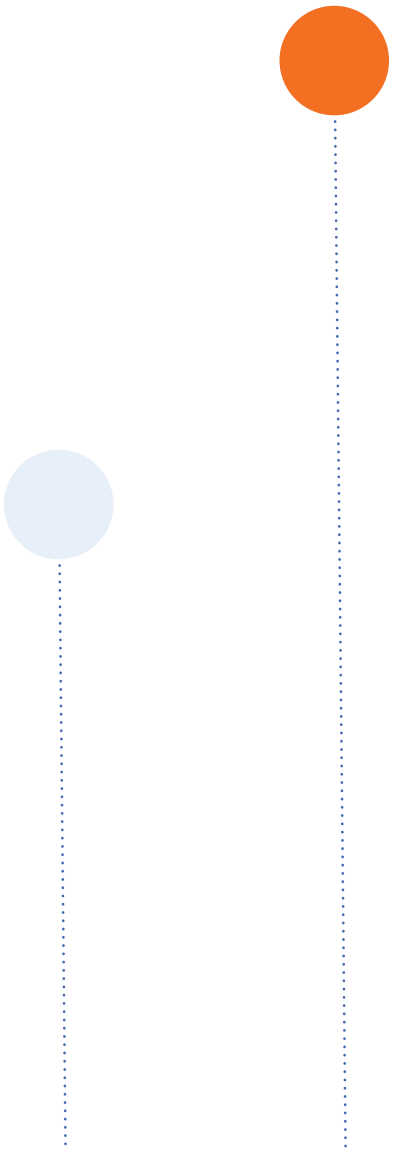
A certificate is a data set providing the technical identity information of the authority and must be digitally signed by the next higher authority in the hierarchy. The process of signing is cryptographic, where a digital signature is generated from the certificate data. This signature is a small amount of data that can be validated using the corresponding public key. Validation ensures that the certificate's data have not been altered, thereby proving the integrity of the data. Additionally, the certificate, combined with the authority's information, confirms its origin.

To validate the origin of a CA, the public key of the next higher CA certificate must be available. The Root CA, however, can only validate itself, as it has no higher authority. Since the Root CA is self-signed, it is critical to ensure that the root certificate is not compromised and originates from a trusted entity.

The entire trust framework is governed by a PKI Policy and Practice Statement, which regulates all principles, structures and implementations. The examples and principles illustrated here are simplified, as the full implementation of a PKI framework requires extensive planning and is highly complex to manage. The security and integrity of the Digital ID system are entirely dependent on the trust model and its PKI infrastructure.

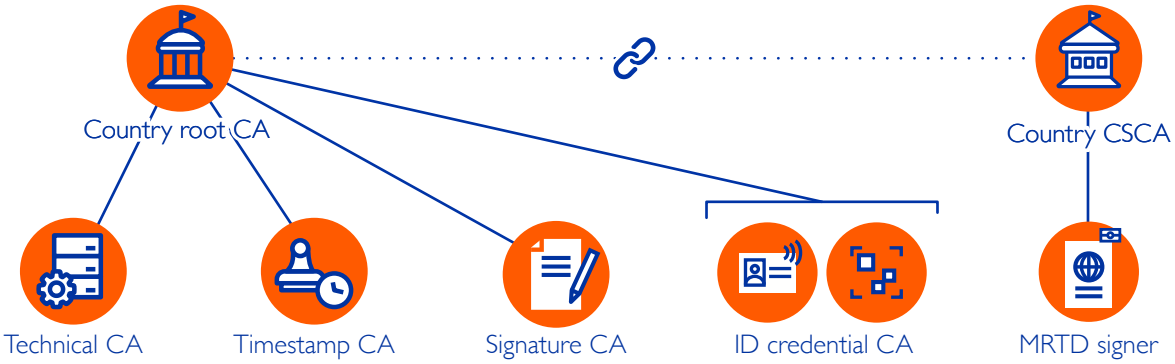
The configuration of the PKI infrastructure must align with the functionality and requirements of the Digital ID system. The provided example serves only as an overview to offer a basic understanding of the requirements and complexity involved.

In some cases, the hierarchy may include multiple Root CAs if different services are operated under separate authorities. In such cases, it is essential to link the CAs, for example, using link or bridge certificates. This is particularly relevant if, simultaneously, travel credentials are issued, which require a separate CA according to the ICAO 9303 standard, referred to as the CSCA (Country Signing Certification Authority). Establishing a trust link between Root CAs is optional but can enhance interoperability.



1.6.4.1 EXAMPLE OF CERTIFICATE AUTHORITIES IN A DIGITAL ID SYSTEM

Figure 19. Example of a Trust Model for Digital ID systems



The different (CAs that can be implemented in a Digital ID System include:

- **Country Root CA (mandatory)**

  The Country Root CA is mandatory and serves as the highest authority in the Digital ID System. The private key is held exclusively by the Digital ID managing entity and must be safeguarded with the highest level of security. The size and strength of the key must always exceed those of subordinate CAs.

- **Technical CA (mandatory)**

  The Technical CA is responsible for issuing technical certificates that secure the communication of servers, interfaces and other technical components within the Digital ID system infrastructure. This CA is mandatory and critical for ensuring the cybersecurity of the system. It may also ensure that only authorized passes are loaded into the user's mobile wallet.

- **Signature CA (optional)**

  The Signature CA is optional and required only if the Digital ID installation supports digital signatures for users. When implemented, this CA issues user-specific signature certificates based on individual private keys, typically managed centrally for remote signatures. Each individual receiving a signature certificate can digitally sign documents using their private key.

- **Timestamp CA**

  The Timestamp CA has the sole function of providing a qualified timestamp. Proof of the exact time when a transaction or signature is performed is crucial for Digital ID systems, as well as for many other IT systems. Time sequencing ensures events occur in the correct order and serves as a key element of evidence.

  The Timestamp CA is linked to a specialized timestamp server, which uses multiple time-referencing systems to provide accurate time signals. Examples of these systems include GPS (US system), BeiDou (Chinese system), GLONASS (Russian system) or Galileo (European system). Other possible time sources include atomic clocks (e.g. cesium based) or, in Europe, the DCF77 transmitter, which distributes a low-frequency time signal across Europe and is based in Germany. A timestamp server typically uses 2–3 synchronized time sources to avoid errors. Upon a server's request, the Timestamp CA signs a transaction with a timestamp, ensuring all devices within the Digital ID system use precisely the same time.

- **ID Credential CA**

  The ID Credential CA signs all digital identity credentials, which can be stored as digital tokens on various media, such as VDS or VC in a QR code or other formats. This CA can also issue individual authentication certificates used by users to access IT systems. In some implementations, authentication certificates for users are managed separately from the ID Credential CA, depending on the managing entity.

To validate the ID credentials of a VDS or chip token, the public certificate of the ID Credential CA is required.

The ID Credential CA can also sign digital credentials stored in mobile device wallets. However, in some implementations, credentials in the wallet may be signed by a different CA. This depends on the issuance model and whether all issuers use the same ID Credential CA or their own. If issuers use their own signing authorities and operate separate ID Credential CAs, these are typically issued under the same root CA for simplicity and security. However, theoretically, they could originate from a different root CA, such as when storing travel documents in the same wallet.

- **ICAO CSCA**

  The ICAO CSCA is a separate root CA used to govern the issuance of international travel documents in a country. It operates under a different policy aligned with the ICAO 9303 standard. According to ICAO requirements, the CA must be a self-signed root CA and is exchanged through the ICAO Public Key Directory (PKD). The CSCA signs the MRTD (machine readable travel documents) Signer CA, which subsequently signs the data in all travel documents issued by the country.

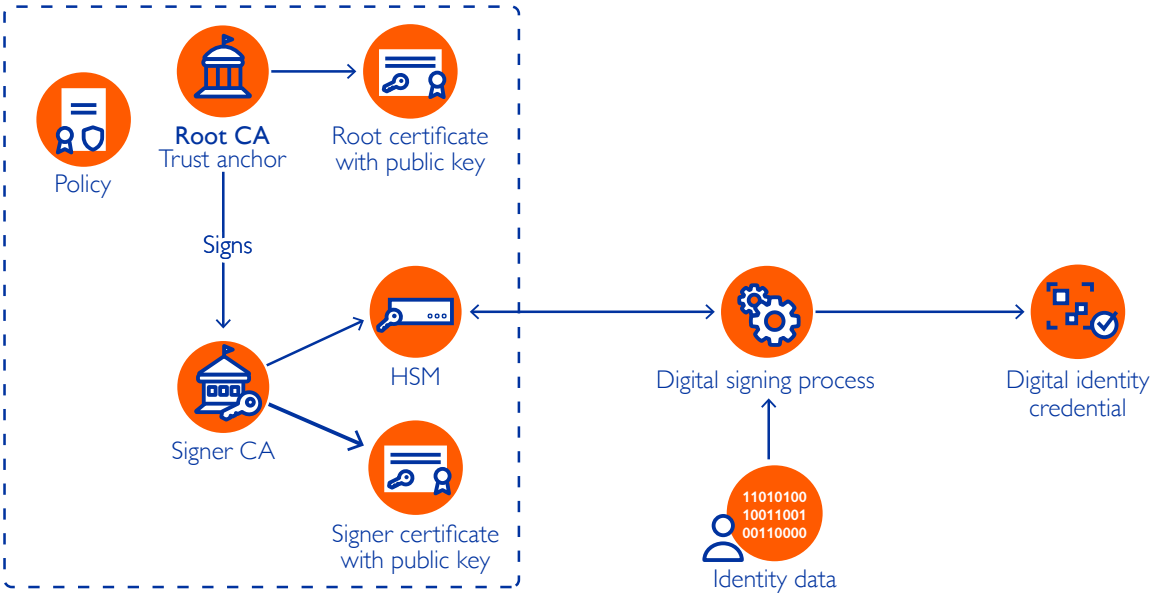
- **MRTD Signer**

  The MRTD Signer, also called the document signer, is responsible for signing the data stored in travel documents, such as passports and ICAO DTCs.

1.6.4.2 DIGITAL SIGNING PROCESS (MAIN EXAMPLE)

The process of signing and validating signatures is fundamentally the same, regardless of what is being signed. In this process, all information is treated as data, which is signed to ensure its integrity and origin. The example in this chapter is simplified and illustrates the signing of a VDS ID credential and its validation.

Figure 20. Digital signing process example on VDS identity credential



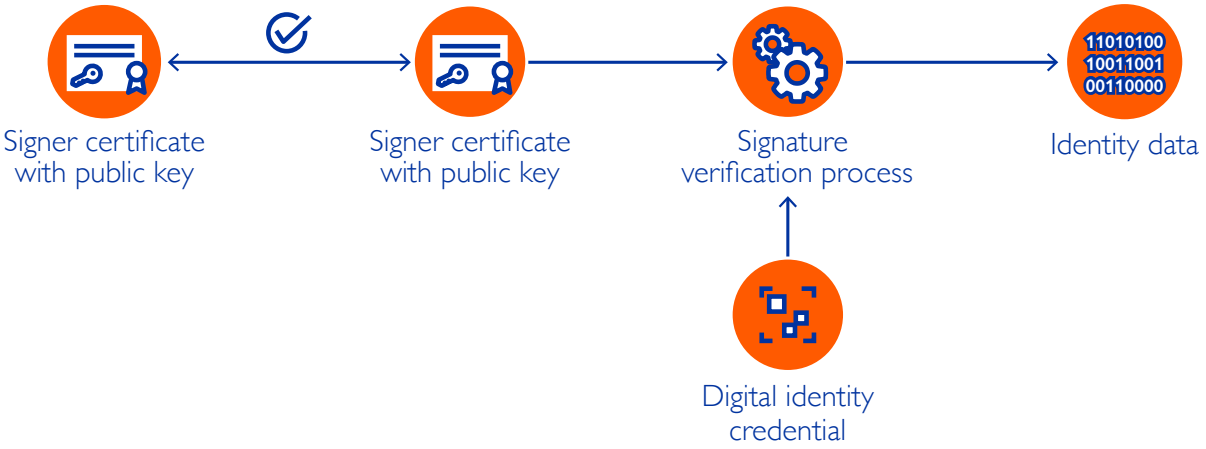
The entity signing the identity data generates a key pair consisting of a private and public key using a HSM. The HSM securely protects the private key digitally. The public key is submitted to the root CA, which incorporates the issuer's identity information and signs the issuer's certificate.

The issuer now possesses a private key stored securely in the HSM and a public certificate that identifies the issuer and links to the private key. During the signing process, identity credential data are prepared by the system and a token is created. The token's format typically follows standards such as ISO 22376 VDS for

visible digital seals or WC3 for internet-related tokens. In a cryptographic signing process, the issuer uses the private key hosted in the HSM to sign the data, and the resulting digital signature is added to the token. For example, the token can be converted into a QR code, which may be printed, displayed on a mobile device or stored as data in a secure chip.

While generating the token, additional data such as the pass's characteristics, validity and other parameters are added to identify their attributes (see 1.2.2 Digital Credentials).

Figure 21. Digital signature verification process



To validate the credential, a verifier must have the following:

- The signer certificate used to sign the credential.
- The root certificate that was used to sign the signer certificate.

It is mandatory for the verifier to ensure that the root certificate belongs to the correct certificate issued by the Digital ID managing entity. It is recommended that the verifier use a certified application from the Digital ID managing entity or ensure access to the correct certificate by obtaining it from a secure and trusted source, such as a Trusted List or PKD.

STEP 1: VALIDATE THE SIGNER CERTIFICATE

The verifier must first confirm that the signer certificate is linked to the correct root certificate. This involves verifying the chain of trust by checking the signature of the signer certificate against the public key of the root certificate.

STEP 2: VALIDATE THE DIGITAL ID CREDENTIAL

To validate the Digital ID credential, the verifier checks the attached signature (a small amount of data representing the digital signature of the credential). If the credential data have been altered, the signature verification will fail. Verification succeeds only if the credential data remain unchanged since they were signed by the issuer.

Upon successful verification of the digital signature, the integrity of the credential is confirmed. Using the data in the signer certificate, the verifier can further confirm whether the issuer is the expected entity, thereby validating the origin of the data.

Security considerations

While the process of digital signing and validation is technically complex, it is fundamentally the same for all digital signatures. A robust policy and practice statement is crucial for the trust framework to ensure the security of the entire system. This policy defines the security measures, handling procedures, auditing requirements and compliance guidelines. Non-compliance with the policy or practice statement by any part of the technical infrastructure or its actors can compromise portions of or even the entire Digital ID system.

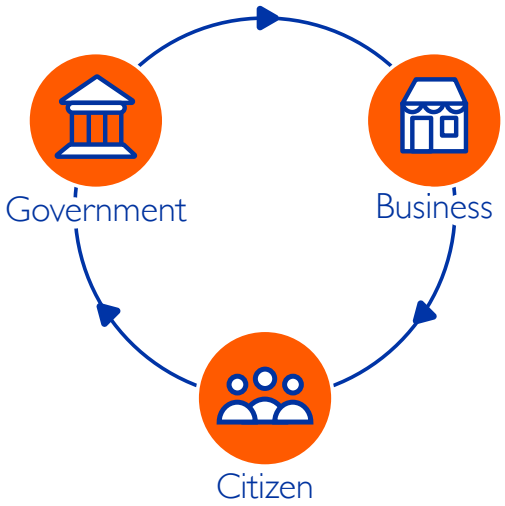
PKI management

The management of PKI systems and processes must be handled with the highest level of attention and diligence by the Digital ID issuing entity.

1.6.5 VISIBLE DIGITAL SEAL TECHNOLOGY

Identity-related documentation has long been used to verify transactions and eligibility. These documents can be presented in various formats, including traditional paper, digital transmissions, or mobile applications. While Digital ID represents one approach, VDS technology serves as a flexible solution applicable to a wide range of document types. The Digital ID toolkit focuses on identity documentation issued by government entities, though private entities can also utilize similar technology for verification in service provision.

Figure 22. Document and ID usage involved



VDS technology enhances inclusive verification through accessible validation processes. To successfully implement Digital ID and VDS in identity documentation, the following critical criteria must be met:

- Electronic processing to ensure easy use in today's digital processes and verification by any entity.
- Security measures to prevent document forgery and identity falsification.
- Data privacy protocols to protect personal information and ensure compliance with local data protection laws.
- User operability to enable access for the global population through available methods.
- Interoperability to facilitate exchange between entities or countries while maintaining flexibility.
- International acceptance, trust frameworks and policies for security and operations.
- Infrastructure availability for VDS issuance and credential verification.
- License-free technology available worldwide to all countries and verifying organizations.

1.6.5.1 DIGITAL TRANSFORMATION

A document issued by a legal entity or authority contains key information that defines and represents it. For legal identity, this typically includes details like name, birth date and nationality. Traditionally, this information is printed on paper. In the digital era, such information is stored in databases as digital records managed by IT systems. To facilitate exchange between entities, these records must be presented in an exchangeable format. In traditional systems, this is achieved through printed documents, while in digital systems, a standardized token represents the equivalent.

A token is a structured set of digital information that is complete, follows an interchangeable format and can be universally interpreted. To ensure data integrity and prevent forgery or accidental alteration, tokens are secured with digital signatures. Digital signatures, based on PKI, enable only the issuer to sign the token, while verifiers use publicly available certificates

to confirm the token's authenticity. This process not only ensures the integrity of the information but also embeds the issuer's identity, providing assurance of the document's origin.

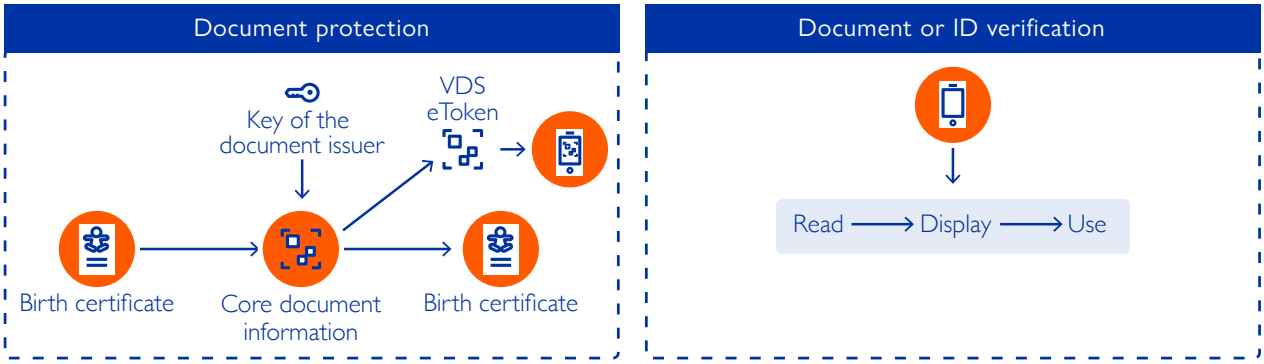
Digital signature technology enables reliable transformation of any information into trusted data within a digital ecosystem. Data secured with a digital signature is referred to as a "digital seal," indicating that the information is electronically sealed. Unlike scanned documents, which may be error-prone and unreliable in confirming their origin, digitally signed tokens ensure secure electronic management, authenticity and integrity. Representing a document as a digitally signed token is a pivotal step in transitioning from paper-based to digital services. Since physical presentation is often still required, digitally signed tokens can also be embedded in printed documents.

VDS technology bridges digital systems and printed or visualized data. To make digital seals accessible in printed or visual forms, they are represented using two-dimensional barcodes. These barcodes can store large volumes of data compactly while remaining machine-readable, making them ideal for this purpose. Although 2D barcodes have storage limitations, they are generally sufficient for representing essential information. When a digital seal is presented as a 2D barcode, it becomes a VDS, providing a visual representation of a digital seal.

The concept of securing and presenting Digital IDs aligns with VDS principles, using digital signatures to verify identity and information. The issuance of a VDS depends on a robust trust framework and PKI policies. The issuer must be an authorized and identifiable entity. This trust framework ensures the validity of the token by connecting the digital signature to the authorized issuer. While generating signing keys is technically straightforward, linking them to a trust framework ensures a high level of trustworthiness and organizational accountability.

Once issued, a digitally signed token (digital seal) can be managed by digital devices like mobile phones or ID systems and presented as a VDS in printed format. VDS technology allows seamless conversion between electronic and printed formats without data loss, maintaining full integrity. Scanned VDS barcodes can be reconverted into complete digital data using specialized software, ensuring consistency across various media.

Figure 23. Visible Digital Seal generation and verification



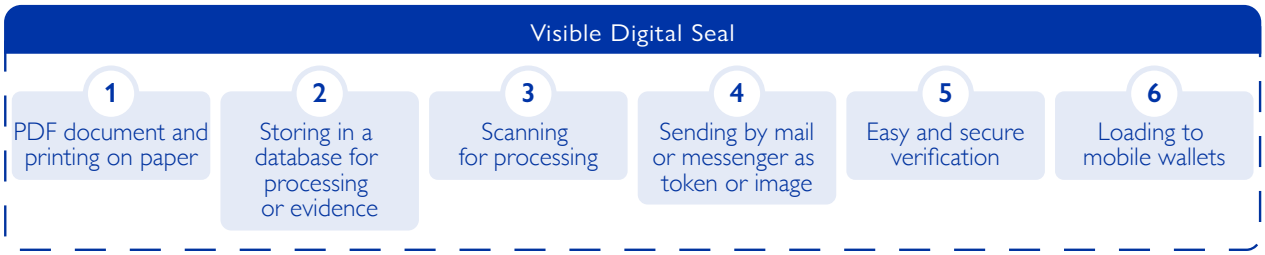
VDS technology is already implemented in applications like visas and electronic proofs, and many countries use proprietary VDS systems for tasks like tax invoices. However, when VDS is used across multiple government applications, standardization becomes critical. The choice of barcode type and encoding method must ensure universal interpretability. A robust trust framework is essential for validation, especially in cross-border scenarios, requiring bilateral or multilateral agreements to manage policies and processes. The European Union's eIDAS regulation exemplifies an interoperable trust framework, enabling digital seals and signatures issued in one European Union country to be validated in others under a unified trust list.

If private entities are included in the trust framework, additional complexity arises, particularly concerning the validation of business licenses to confirm their legitimacy. To maintain simplicity and security, government trust frameworks for issuing Digital IDs and VDS are often kept separate from those used

by private entities. This separation ensures a clear trust anchor for citizens and easier maintainability of government systems. While private entity trusts frameworks enhance overall societal digitalization, they are best managed independently under similar technical standards but separate policies.

The presentation of digital identity follows the schema of a digital seal, embedding identity information and securing it with the digital signature of the responsible government entity. This approach ensures secure and trustworthy management of identity in the digital environment.

Figure 24. Visible Digital Seal usage options



The trust framework is a key factor for the validation in generic VDS schemes. If a trust framework includes public and private entities, an additional layer of complexity is added. The same applies if a trust framework shall operate across the country's borders, which requires a bilateral or multilateral agreement, adding an additional organizational complexity regarding policy and processes.

1.6.5.2 CROSS-BORDER INTEROPERABLE TRUST FRAMEWORKS FOR VISIBLE DIGITAL SEAL

A good example of an interoperable trust framework for digital seals is the eIDAS regulation in the European Union, supported by the European Union Trust List. Each country certifies its PKI, which becomes part of a European Union-wide trusted list. This framework enables a digital seal or digital signature issued in one country to be interpreted and validated in another. The foundation of this system is unique, as it is built on European Union legislation that applies uniformly across all its Member States.

Establishing a comparable scheme in other regions is more likely to occur through bilateral agreements. The regulation traces its origins to the first European Union Signature Directive from 1999,[13] reflecting a development period of 25 years leading to the current eIDAS regulation.

A less complex alternative is an in-country implementation, which does not operate across borders and offers only limited cross-border functionality through bilateral agreements, such as the IOM use case described in Part 3 of this toolkit.

ICAO PKD

Another example is the ICAO PKD, a trust framework and trusted certificate exchange platform that operates across borders. The ICAO PKD enables countries to obtain digital certificates for verifying electronic passports, their digital credentials and ICAO VDS documents.

13 European Union. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (Brussels, 1999).

ISO 22385 VDSIC trust framework

To ensure security and interoperability, ISO standards define a method to centralize useful resources, such as the Manifest. These resources are organized in a Trust List, a signed XML file that inventories Trust Service Lists (TSLs). Each TSL lists authorized operators (TSOs) and authorized CAs and references the URL where the Manifest and public certificates can be retrieved during the verification process.

Each element supporting the Otentik VDS (such as Trust List, TSL) is protected and signed by the TSO. To ensure service reliability, verifying the various elements of the Otentik VDS and maintaining the chain of trust is essential. To manage trust across a network of heterogeneous use cases and actors while preserving the sovereignty of trusted entities (such as States, the Otentik network), the concept of subnetworks of trust is necessary.

The root of trust is established by the Otentik Trust Network, which provides a Trust List. This Trust List defines each subnetwork and identifies a management entity responsible for maintaining trust within its scope.

Each management entity must provide a TSL and a practical statement for all trust actors operating within the subnetwork. The identity of every signatory entity (TSP) must be strictly standardized and verified (such as eIDAS, WebTrust for CA, State CA) to ensure trust and legitimacy. Furthermore, a TSP is authorized to sign only predefined and approved use cases.

Private entities

If a trust framework includes private entities that are non-governmental, it must take into account the business license issuing authorities in the country. Any entity issuing a document or identity in the form of a VDS or digital seal must be part of a trust framework. Without a trust framework, a digital seal or document can be issued but only gains validity through the framework, as the latter provides proof of the document's or seal's origin.

The trust framework serves as the digital link between the legislation that authorizes an entity to issue a valid document and the digital representation of that document in the form of a digital seal or VDS. Only when a verifier can clearly determine the origin of the data can it validate whether the issuing entity is authorized to issue that type of document.

If a trust framework includes private entities, it must also be linked to the business license authority to confirm that a business is legally registered. However, the inclusion of private businesses in a trust framework adds complexity to a government system, and it is generally advisable to avoid doing so. Information and seals for private entities can be issued using a technically similar standard but managed within a separate trust framework. While both frameworks can be based on legislation governing digital documents and infrastructure, they should remain separately managed in terms of policy and trust.

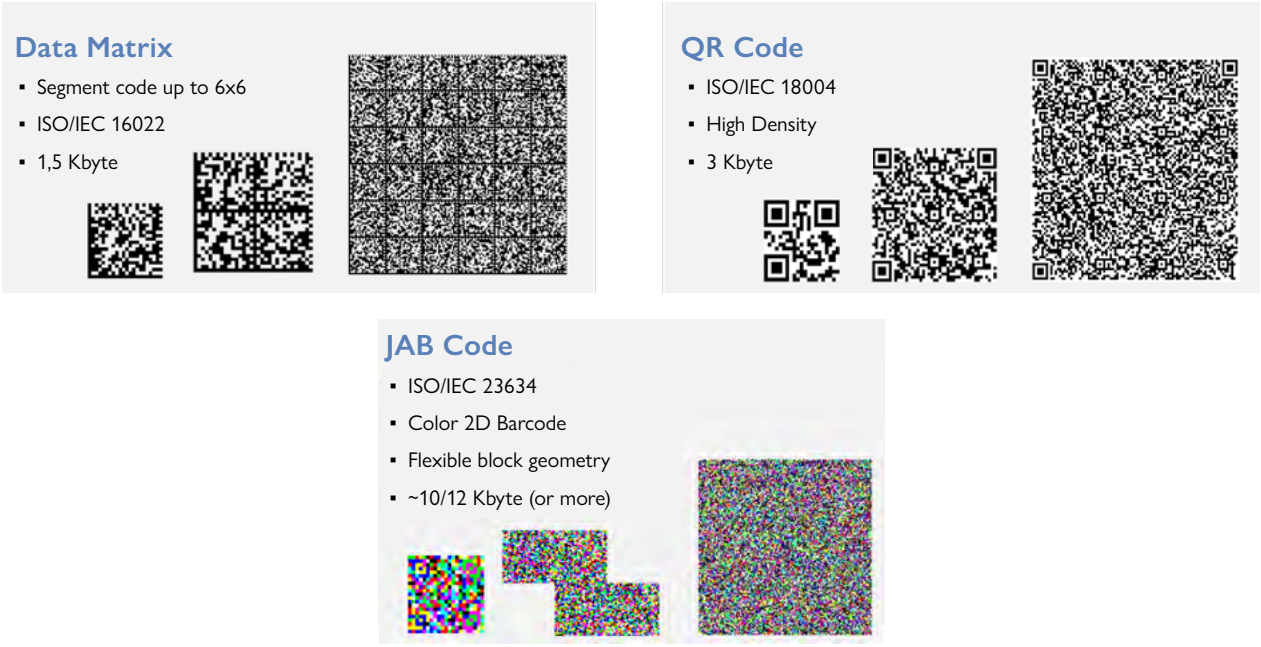
Keeping the trust framework for government entities separate – particularly for the issuance of Digital IDs – ensures a higher level of maintainability and establishes a clear trust anchor for citizens. Nevertheless, a trust framework for private entities can significantly enhance and enable broader digitalization across all areas of life.

This toolkit focuses on the management of a trust framework used exclusively by government entities for the issuance of Digital IDs and documents. These documents can still be validated by government entities, private businesses and citizens.

1.6.5.3 STANDARDS FOR VISIBLE DIGITAL SEALS

To ensure the readability of VDS, the presentation of 2D barcodes follows common ISO standards such as ISO 18004[14] for QR codes and ISO 16022[15] for Data Matrix codes. These barcodes can store a considerable amounts of data – up to approximately 3,000 characters for QR codes, depending on the parameters used. Mobile phones and other barcode readers with cameras can process and read QR and Data Matrix 2D barcodes, which are then automatically converted to digital seal data.

Figure 25. Visible Digital Seal 2D barcode standards



The way data for digital seals or Digital IDs are encoded into a 2D barcode follows various standards. In some cases, the data representation in 2D barcodes is proprietary and linked to specific vendors. To maintain system independence from vendors and avoid reliance on proprietary technologies, international standards have been developed.

ICAO9303 Visible Digital Seal standard

For travel documents such as passports, ICAO has specified a format and related use cases in the ICAO 9303 Part-13 standard, which includes visas, electronic travel approvals and temporary passports. ICAO's approach is focused on travel-related use cases and does not specify general methodologies. The ICAO 9303 VDS standard utilizes the ICAO-PKD trust framework for signing the data used in VDS.

The ICAO VDS is designed for compact barcodes in Data Matrix format. The data are fully binary, which can make interpretation challenging for some applications. While binary barcode data representation is part of the ISO standard for QR and Data Matrix barcodes, it is not widely implemented in many devices.

The largest application of ICAO VDS is the Schengen Visa, with other use cases including Electronic Travel Authorizations (ETA).

14 ISO. ISO/IEC 18004:2024. Information technology — Automatic identification and data capture techniques — QR code bar code symbology specification (ISO, 2024).

15 ISO. ISO/IEC 16022:2024(en). Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification (ISO, 2024).

ISO-22376 VDS standard (Otentik VDS)

Another international standard is ISO 22376, which specifies all aspects of a VDS standard in a comprehensive and systematic way. The standard supports multilingual characters and flexible data structures. The standard describes various use cases and a model for exchanging digitally signed VDS description manifests, along with a trust framework and the VDSIC trust framework (ISO-22385).

ISO 22376 is maintained by the Association Internationale de Gouvernance du Cachet Électronique Visible, based in Paris, France.[16]

Otentik VDS is a structured data set, often in the form of a machine-readable code, used to ensure the authenticity and integrity of key data associated with documents or objects. Otentik VDS provides a cost-effective solution with high security, helping to combat document forgery and, when necessary, verify peoples identities through biometric recognition, while maintaining privacy.

Otentik VDS is based on open standards ISO 22373 and 22385 and operates within the Otentik Trust Network. This network ensures the authenticity and legitimacy of documents, objects and goods, connecting verifiers with those authorized to certify them.

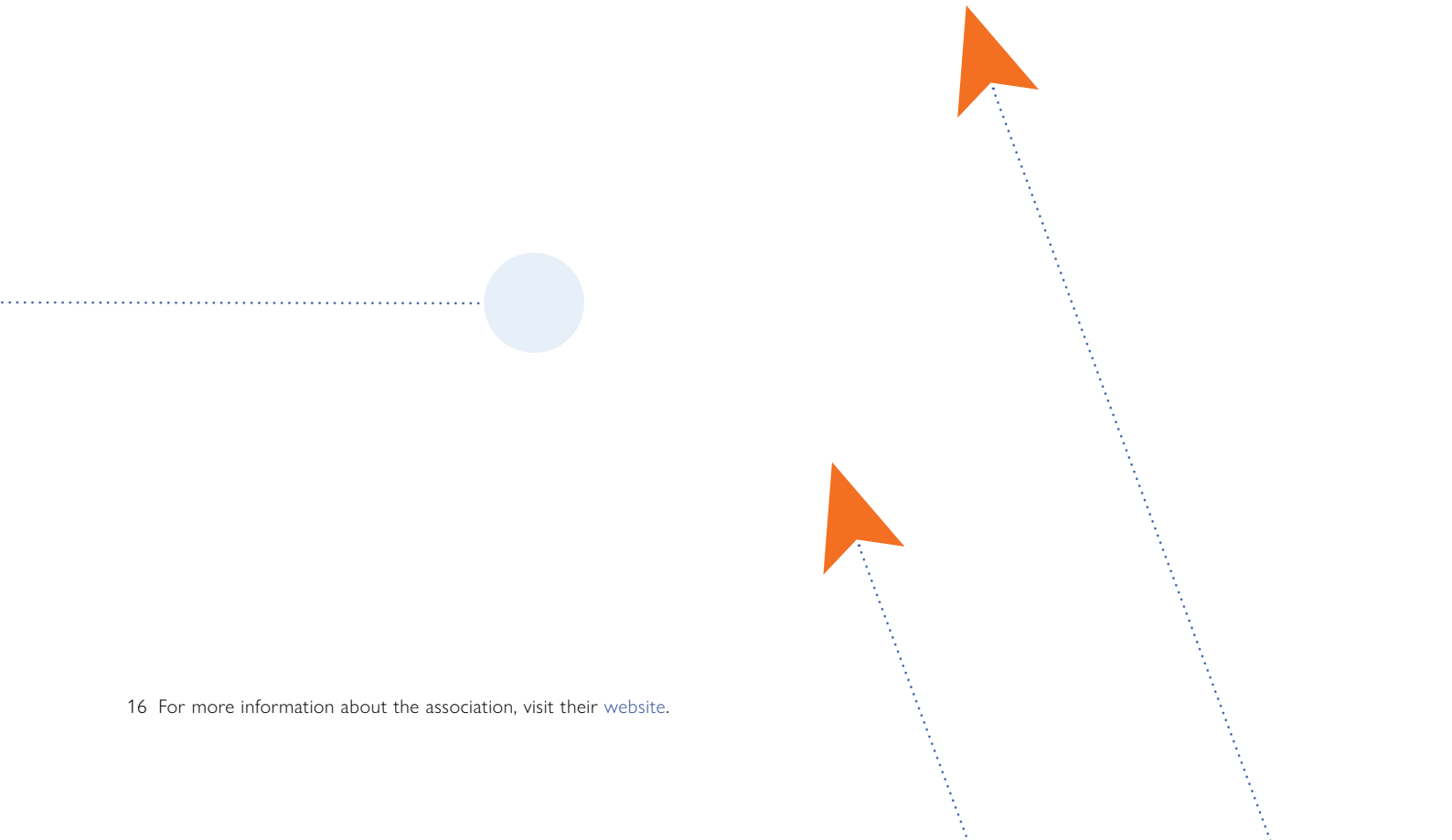
General concept

The Otentik VDS is always tailored to a specific use case defined by a group of experts. Each use case determines the key data fields to be included in the schema, along with the field constraints. If necessary, the use case may also specify additional verification policies such as authorized symbologists, signer legitimacy, validity period, Presentation View and post-verification business rules outlined in TSO extensions. Use cases are converted into a secure XML-format file (the Manifest).

Issuers and verifiers of the Otentik VDS can interpret and process the Manifest in a standard, deterministic way, adhering to the rules defined for each use case.

Electronic signature

Many steps allow to minimize the amount of space used by the data carrier and to maximize the amount of space available for data. As such, the Otentik VDS does not contain the certificate used for the signature nor the definition of the use case but contains identifiers allowing for their retrieval.



16 For more information about the association, visit their website.

1.7 CHALLENGES FOR DIGITAL IDENTITY SOLUTIONS

While Digital ID offers numerous advantages, such as reducing service costs and enhancing services for citizens and residents, its implementation presents several challenges that must be effectively addressed. These challenges span the entire implementation process, from meeting initial prerequisites to ensuring continuous improvement and maintenance of systems.

The key challenges, as outlined in the toolkit, include:

1. Governance of Digital ID;
2. Legal framework and legislation;
3. Digital maturity and readiness of identity management and registration;
4. General digital infrastructure;
5. Scalability of technical Digital ID systems;
6. Use case planning and key applications;
7. Marketing and user participation (onboarding rate);
8. Business model and financing.

1.7.1 GOVERNANCE OF THE DIGITAL ID

Digital ID is a relatively new concept in the country and plays a crucial role in its broader digitalization efforts. It serves as a cross-cutting initiative that interacts with various government digital services and platforms, particularly those responsible for civil registration and the issuance of traditional identity documents such as e-passports and ID cards used for travel.

Unlike traditional identity documents, the legal and regulatory framework for Digital ID systems is often underdeveloped or not explicitly defined, as these technologies evolve alongside their implementation. The success of a Digital ID system largely depends on the governance model and the distribution of responsibilities within the Government. Governments must decide whether to integrate Digital ID within existing infrastructure or create a dedicated entity such as a government-owned semi-private organization. This decision must account for the specialized technical expertise required, which is in high demand from both public and private sectors.

The governance model must support the recruitment and retention of skilled resources while ensuring balanced oversight across the involved government entities. Doing so is particularly important when Digital ID is part of a federated identity (SSO framework. Digital ID governance should also be backed by strong legislation, ideally covering mandates such as digital signatures and PKI operations.

A well-defined governance structure is essential for clarifying the responsibilities of the agency or government entity tasked with implementing and managing the Digital ID system. Coordination among various government bodies may pose political challenges, but these can be mitigated by establishing supporting laws, policies and clearly defined roles and responsibilities for Digital ID implementation, management and operation.

While creating a new entity to oversee Digital ID is not mandatory, doing so is often the most effective solution. Extending the mandate of an existing authority may introduce complexities, leading to delays and increased costs. The governance approach should be tailored to the country's context, considering its governance structure and historical factors. Typically, the entity responsible for implementing Digital ID is created at the top level of government.

Once governance is established, the next critical step is to develop a comprehensive Digital ID road map and implementation framework, which includes assessing the country's digital maturity, existing infrastructure and planning for practical use cases. Careful planning and coordination are vital for the successful rollout of Digital ID systems, ensuring alignment with the nation's digital transformation goals.

1.7.2 LEGAL FRAMEWORK AND LEGISLATION

The legal framework presents a considerable challenge, as it demands specialized expertise that may not always be readily available, as well as the approval of legislative bodies or other relevant decision-making authorities. Establishing this framework begins with a thorough understanding of the existing regulations governing digitalization within the country. These regulations must be reviewed and augmented to support the implementation of a Digital ID system effectively.

A comprehensive legal framework can be initiated with a general act that addresses the digitalization of government processes. This act can then be supplemented by detailed bylaws and policies tailored to the specific needs of Digital ID implementation. Integral to this framework is the governance structure, as previously outlined, which serves as a critical factor in ensuring the success and sustainability of the Digital ID system.

1.7.3 DIGITAL MATURITY AND READINESS OF IDENTITY MANAGEMENT AND REGISTRATION

A key prerequisite for successfully implementing a Digital ID system is the country's digital maturity and the readiness of its identity management and registration systems. Digital maturity begins with the registration of legal identities and life events such as births in a civil registry. The percentage of the population with registered legal identities is a key indicator, as participation in a Digital ID system is impossible without this foundational step.

The next stage is the maturity of identity management. Digital IDs are typically issued to individuals who have reached the legal age defined by the country's regulations, commonly 18 years but possibly varying (in some countries, 16 or 21 years). A critical indicator of readiness is the proportion of the population registered in a national database, which assigns unique ID numbers or similar identifiers. The system must also support biometric data capture and deduplication processes to ensure unique identities. Biometric databases are essential for guaranteeing identity uniqueness and enabling biometric verification. Mandatory biometric data include high-quality live-captured photographs, fingerprints and optionally, iris scans. Systems capable of managing multimodal biometrics provide stronger identity assurance. Digital maturity is reflected in the effective operation of an identity management system and the enrollment of a significant portion of the population.

Without a robust identity management system and related registry, implementing a Digital ID system carries a high risk of failure. To assess readiness, IOM offers a Digital Maturity Assessment Tool[17] as part of its efforts to support the digitalization of identity management of Member States. This tool helps evaluate a country's preparedness by considering factors such as population enrollment, registration systems and digital infrastructure. Both identity management systems and digital infrastructure are critical for the successful deployment of a Digital ID system.

1.7.4 GENERAL DIGITAL INFRASTRUCTURE

The overall digital maturity of a country reflects the availability of infrastructure that enables citizens, residents and government entities to implement and access digital services effectively. The IOM Digital Maturity Toolkit provides a comprehensive assessment framework to generate a digital maturity indicator.

One critical factor is the availability of internet connectivity and the penetration of smartphones among the legally eligible population. However, challenges persist in certain regions, particularly among older demographics or those residing in remote areas. Prior to implementing a Digital ID system, a thorough assessment should be conducted to determine the proportion of the population that can be effectively reached.

Even in regions with lower digital maturity, a Digital ID system can still deliver significant benefits. For remote areas, where traditional services often require residents to travel long distances to access government facilities, a Digital ID system can enhance accessibility and efficiency. This capability underscores

17 IOM, *Migration Management Digital Maturity Assessment Report - Armenia* (Geneva, IOM, 2023).

the transformative potential of Digital ID systems in bridging service gaps and fostering inclusivity, even in less connected regions.

1.7.5 SCALABILITY AND USABILITY OF DIGITAL ID SYSTEMS

The implementation of a Digital ID system and its associated IT infrastructure demands a strong focus on functionality and usability to ensure seamless user experience and successful delivery of the intended use cases. Software performance and use case testing are critical in this regard, as malfunctions or errors can lead to user frustration and broader negative consequences. Issues such as adverse media coverage, unfavourable online reviews, political backlash or outright rejection of the system by users can significantly undermine the initiative, potentially resulting in partial or complete failure.

A key aspect of usability is ensuring the scalability of the system to handle an increasing number of users without compromising performance. While a system may function well with a limited user base during its initial stages, it may face serious challenges during peak usage periods. For instance, government deadlines can cause significant surges in usage, as seen during the rollout of COVID-19 passes in some countries where high demand led to system slowdowns or crashes. Proper predictive analysis and planning, supported by scalable IT architecture and sufficient resources, are essential to mitigate such risks and ensure smooth system operation during peak times.

Service availability is equally critical, requiring the infrastructure to function reliably across the entire country, including remote and poorly connected areas. The system's bandwidth requirements must align with the slowest available internet connections to include as many users as possible. Applications or websites requiring large data transfers, such as high-resolution images or graphics, may become unusable in regions with weaker internet connectivity, thereby excluding certain populations. By optimizing the system for use under all available communication circumstances, the risk of excluding users in remote or less-developed regions can be minimized.

To ensure widespread accessibility and adoption, the Digital ID system must be robust, scalable and capable of delivering reliable services under varying conditions. This approach not only guarantees inclusivity but also builds trust and acceptance among users, which are essential for the long-term success of the initiative.

1.7.6 USE CASE PLANNING AND KEY APPLICATIONS

During the digital maturity assessment, use case planning plays a critical role in identifying applications and services that can deliver the greatest benefits to the population. As the Digital ID system evolves, its applications and service offerings expand alongside the growth and enhancement of digital infrastructure. A significant challenge during this phase is evaluating potential use cases and developing an implementation road map that generates quick wins for both the population and participating government entities.

The implementation of a Digital ID system is not a one-time effort but a continuous process that progresses in tandem with the digitalization of government services. Achieving full rollout and widespread adoption often requires 5 to 10 years, depending on the scale and complexity of the initiative. This extended timeline underscores the importance of careful planning and phased execution to ensure sustainable growth and effectiveness.

One of the main challenges in this process is ensuring ease of implementation and maintenance. A Digital ID initiative should start with a proof of concept and a pilot project focused on a key application. This phased approach allows for initial testing and refinement while also providing early opportunities for user onboarding. Simplicity in the initial features and functionality is critical, as overly complex or non-intuitive interfaces can discourage adoption and create barriers for first-time users. By linking the Digital ID to a straightforward yet essential service, users are more likely to engage with and adopt the system.

Once users are onboarded, the Digital ID platform can evolve through automatic updates and the introduction of new services. The first-use experience is pivotal; users need to immediately recognize how Digital ID simplifies their lives. This positive initial experience helps build trust, fosters adoption and highlights the tangible benefits of the system, ultimately supporting the broader goals of the initiative.

1.7.7 MARKETING AND USER PARTICIPATION (ONBOARDING RATE)

Monitoring the performance of Digital ID systems and defining KPIs are crucial to assessing system usage and user acceptance. If acceptance is low and users fail to perceive clear personal benefits from using Digital ID, the system will struggle to gain traction and achieve widespread adoption. To address this challenge, supporting the implementation of a Digital ID with a well-planned marketing and information campaign is essential. This campaign should be closely aligned with KPI outcomes, initially focusing on user onboarding rates and early usage patterns.

A primary objective during the initial phase is to ensure users install the Digital ID app on their smartphones. Once onboarded, the first-use experience becomes critical. A negative user experience at this stage can undermine adoption efforts. If negative feedback is identified, the system must be promptly adjusted and the media campaign should communicate these improvements in a positive and reassuring manner to rebuild user trust.

One strategic opportunity to introduce users to Digital ID is during the issuance of new national ID cards. This provides a natural entry point for users to engage with the system. Linking the Digital ID to national ID cards can streamline the onboarding process and enhance authentication through integrated features. However, doing so requires careful coordination between the Digital ID rollout and the national ID card programme.

The introduction of a Digital ID may also influence the design and functionality of existing national ID cards. As certain features traditionally embedded in the card transition to the Digital ID platform, there is potential to reduce the complexity and cost of national ID card programmes. This shift can be a compelling financial incentive for implementing Digital ID systems. For countries without existing national ID schemes, the introduction of a Digital ID offers the opportunity to significantly reduce the technical and electronic requirements of physical ID cards, potentially achieving substantial cost savings and operational efficiency.

1.7.8 BUSINESS MODEL AND FINANCING

Digital ID implementations offer significant indirect benefits by reducing the costs associated with providing digital services for government entities. These cost savings arise from lower process and IT expenses, as a shared Digital ID framework enables entities to rely on a centralized identity infrastructure. Furthermore, Digital ID facilitates the digitalization of government operations, replacing manual and paper-based processes with automated, streamlined solutions. For citizens, the benefits include continuously available services, faster processing times and greater convenience. However, while the monetary savings for government entities can be challenging to quantify, the advantages for citizens are often reflected more in terms of improved user experience and less in direct financial gains. Overall, Digital ID supports societal modernization and inclusivity.

Despite these benefits, financing Digital ID implementations, particularly identity management solutions, remains a considerable challenge. Initial implementation costs (CAPEX) can be substantial, while the return on investment is often gradual. In addition, ongoing operational costs (OPEX) must be sustained, requiring funding through government budgets or an internal business model. While CAPEX may sometimes be covered by grants or external funding, OPEX demands continuous budgetary support to ensure long-term sustainability.

Implementing a business model that involves direct service-based payments from citizens often discourages adoption, as it creates a barrier to usage. Some countries have experimented with charging citizens for digital signatures or authentication services, but these models tend to limit user adoption and fail to deliver the widespread cost-reduction benefits that Digital ID systems can achieve.

To address these challenges, governments may explore various funding strategies. For instance, while CAPEX could be financed through donations or grants, OPEX could be supported by reallocating existing digitalization budgets across government entities or directly from central government funds. Alternatively, a usage-based model could be introduced, where government entities pay the central identity provider

based on their use of the Digital ID service. However, this approach carries the risk that entities might avoid using the service to reduce their costs, undermining the system's effectiveness.

Legislation can play a crucial role in ensuring widespread adoption and financial sustainability. Mandating the use of centrally managed Digital ID services by all government entities can help mitigate the risks of non-participation. Additionally, clear financial planning and cross-entity coordination are essential for developing a viable funding model that supports both the initial implementation and long-term operation of the Digital ID system.

1.8 BEST PRACTICES IN DIGITAL IDENTITY MANAGEMENT

This section provides an overview of best practices in digital identity management, focusing on the importance of security and user experience. It covers user experience best practices for digital identity solutions, including usability and accessibility.

Around the world, countries have implemented Digital Identity Solutions that serve as examples of functionality and offer practical guidance on implementation. This chapter highlights successful implementations, with information sourced from local authorities responsible for digitalization and digital identity. The following questions form the basis for analysing Digital ID implementations.

Information capture of Digital ID examples

Considerations for Digital ID systems

a. Stakeholders, operating entity and involved government entities and participating entities

b. Technical understanding of the solution and/or background

c. Functionality – present and future

d. Use cases implemented / key use cases

e. Usage and benefits for citizens and Government

f. Challenges during implementation and operation

g. Operation models / cost (for citizens)

h. KPI's, such as usage, number of users and transactions, others

i. Which entities can use the Digital ID, only Government?

j. Will Government-regulated business such as insurance companies and banks participate?

k. What is the process to bind a mobile to the Digital ID?

1.8.1 BRAZIL'S NATIONAL DIGITAL ID

a. Stakeholders, operating entity and involved government entities and participating entities

The Secretariat of Digital Government manages, funds and provides the platform, relying on databases from various government bodies and private entities, such as the Superior Electoral Court, National Traffic Department, banks, PKI and the new national identity card. Serpro, a public IT company, serves as the technological operator, responsible for the development and maintenance of critical government systems. The platform is available for use by any public body at all levels and branches of government, free of charge.

Most relevant legal instruments:

- **Presidential Decree 8936/2016 -** Establishes the Government of Brazil (gov.br) Platform and the user's unique digital access mechanism to public services.
- **Federal Law 14129/2021 -** Provides principles, rules and instruments for Digital Government.

See here for more information on the Government of Brazil Digital ID initiative.

b. Technical understanding of the solution and/or background

The digital ID is classified into bronze, silver and gold levels, with citizens required to reach a specific level to access desired services.

The bronze level is granted to citizens who create an account and validate personal data held by the Internal Revenue Service, Social Security Service or National Traffic Department. This level allows access to most services on gov.br.

The silver level is granted to citizens who use facial biometrics to confirm identification based on the driver's license database, validate data through internet banking (in partnership with major Brazilian banks), and public servants through their institutional login, in addition to the bronze level requirements.

The gold level is granted to citizens who use facial biometrics to confirm identification based on the electoral justice database, validate personal data through Gov.br by reading the national ID QR Code, or through the official PKI (ICP-Brasil).

The platform operates on a SSO scheme to access public services, offering security features like 2FA by email and mobile number, facial biometric validation and device management.

The software has been developed in-house.

c. Functionality – present and future

Currently, the platform allows citizens to create a digital identity based on formal national identification processes.

A Brazilian national can use many different documents to identify themself in Brazil. The main document is the general registry, issued in each of the 27 Brazilian states, but that has no data interoperability. Using a driver's license, passport or electoral data to create a digital identity is also possible. A new identification process is currently being expanded, which is now unique and national, and is already integrated with digital identity. More than 16 million Brazilians have already issued the new national identity card.

Once created, the digital identity can be used to authenticate across over 4,500 public services. The app enables users to perform biometric validation for digital live proof (starting from 2025 with biometric fingerprints where a photo from the fingerprints is taken live), electronically sign documents (remote server-based signature), receive government notifications (government-to-citizen mail channel and broadcast messages), manage personal data and control security mechanisms like 2FA and device management. Future developments include fingerprint biometric validation through the app, the use of WebAuthn (passkey) and electronic power of attorney. One challenge in Brazil is digital literacy. Many citizens need the support of another person to interact with digital services. This functionality will make it possible for someone to access a service on behalf of another, but with control over who is accessing.

d. Use cases implemented / key use cases

- Provide digital live proof to ensure continued receipt of social and pension benefits without visiting a government office.
- Simplified submission of income tax returns.
- Free electronic signatures.
- Remote application for social and pension benefits.
- Digital access to various documents, including driver's licenses, vaccination certificates, military certificates, work cards and educational declarations. The documents are available in a wallet on the gov.br app, but the user must use a silver or gold digital identity level to access the document.

e. Usage and benefits for citizens and government

A centralized platform for citizen identification and authentication has helped public bodies save resources by eliminating duplicate solutions. It has also accelerated digital transformation, making new digital services immediately accessible through a single personal credential. The centralized solution provides a unified and user-friendly interface, simplifying navigation across thousands of digital services. Moreover, implementing new technologies at one central point enhances value and security for millions of Brazilians simultaneously.

f. Challenges during implementation and operation

Challenges include ensuring scalability to accommodate both public and private services (planned for 2025), tackling the challenges arising from a diverse population with varying social characteristics, and balancing usability with security. Additionally, ensuring that individuals with low digital skills and limited connectivity can fully benefit from the digital identity is another challenge.

g. Operation models / cost (for citizens)

The service is provided free of charge to both citizens and government agencies that wish to integrate it into their systems. The costs are centralized in the Secretariat of Digital Government, which is responsible for driving digital transformation in the federal government.

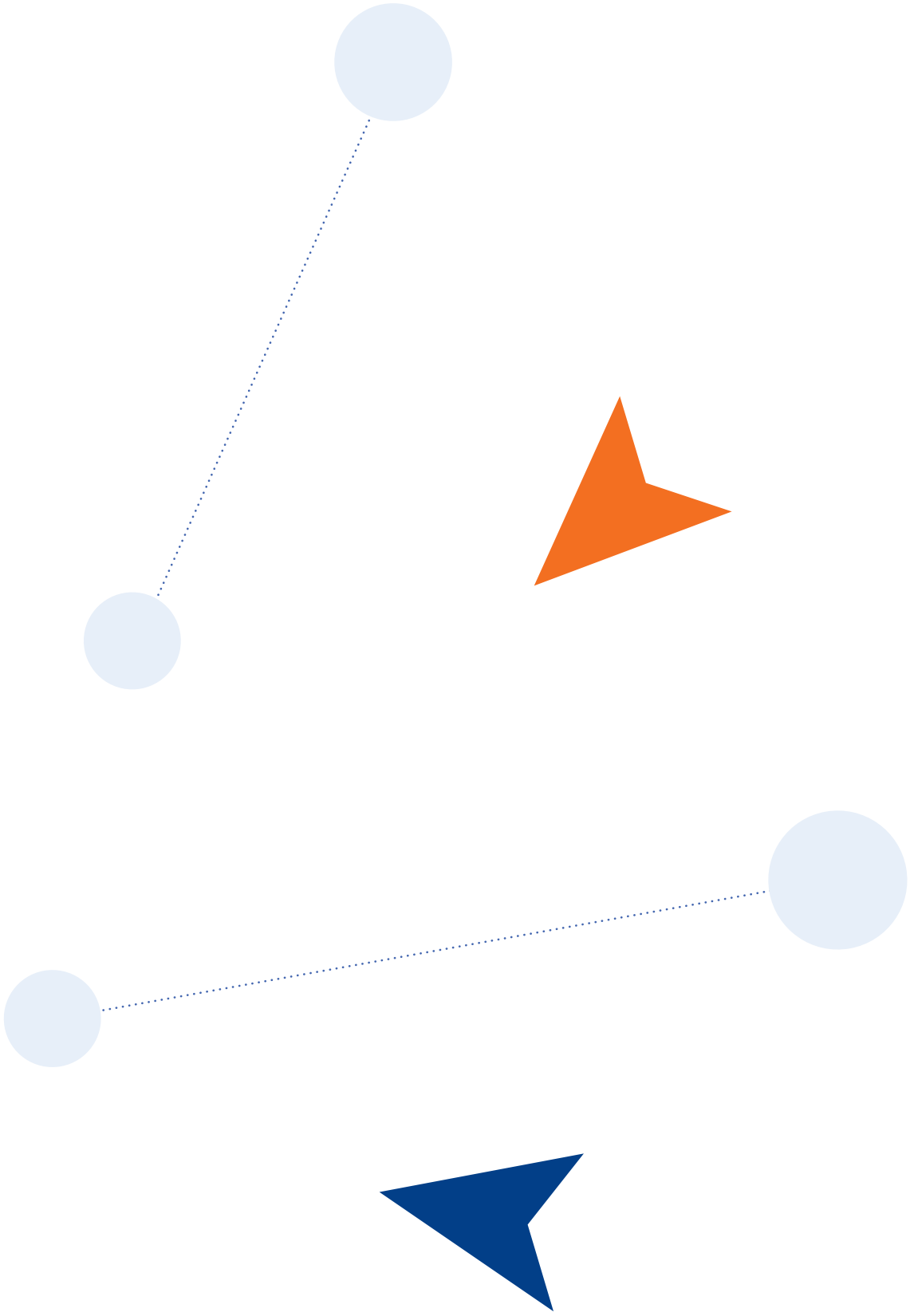
An annual budget is set in the national budget for digital transformation, and part of this budget is used for digital identity. The budget is increasing every year, but as a cloud solution, its growth is slowing as the number of users rises.

To expand into private services, defining a value to be charged to help sustain the platform will be necessary.

KPI's – such as usage, number of users and transactions and others[18]

- Total users: 160.5 million
- Account levels:
  - Bronze: 72.1 million
  - Silver: 27.9 million
  - Gold: 60.5 million
- Monthly authentications: 300 million
- Integrated systems: ~2,800
- Integrated services: ~4,500
- Active app users: 60 million

18 Data were collected in November 2024.



PART 2

Digital Identity Implementation Guidance

Part 2: Digital Identity Implementation Guidance

2.1 GOVERNANCE AND GENERAL GUIDANCE

The chapter contains general guidance to a Digital ID implementation.

- Project setup
- Analysis and information gathering
- Stakeholders of the project
- Application and use-cases
- Legal requirements
- Financing and business plan

2.2 TECHNICAL CONSIDERATIONS FOR DIGITAL IDENTITY

The chapter contains technical aspects of the implementation.

- Existing infrastructure and gap analysis
- Design architecture and development
- MOSIP: A generic example
- System operation

2.3 DIGITAL IDENTITY USE CASE PLANNING

The chapter contains planning of Digital ID use cases.

- Initial use cases
- Implementation road map
- Strategic planning

2.4 COMPLIANCE CONSIDERATION

The chapter contains general compliance considerations.

- Data protection and privacy
- International regulations and human rights

2.5 NON-COMPLIANCE CONSIDERATIONS

The chapter contains non-compliance considerations that should be addressed.

- Customer satisfaction
- Regulations and standards
- Cost
- Quality
- Continuous improvement

2.6 COMPLIANCE RISK MANAGEMENT AND MITIGATION

The chapter highlight compliance risks and their mitigation.

- Compliance assessments
- Quality assessments
- Risk management
- Security controls

INTRODUCTION

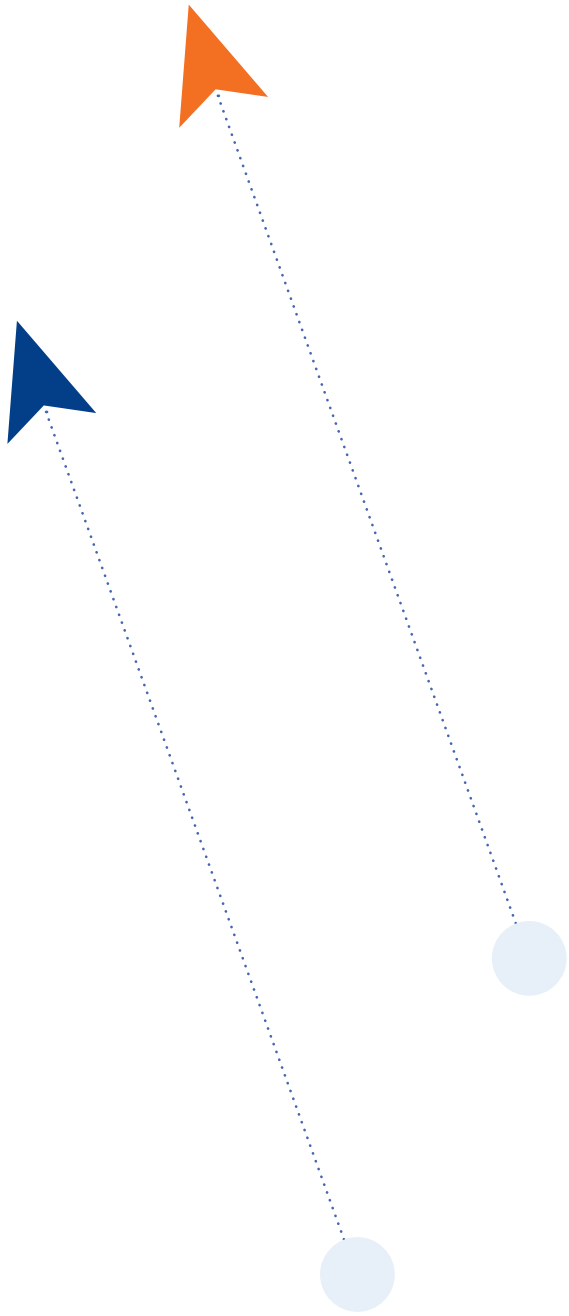
Part II of the IOM Digital ID toolkit provides a practical framework for implementing digital identity systems. Recognizing that each Digital ID project is unique and influenced by local governmental structures, this guideline offers a general approach to navigating the complex landscape of digital identity implementation.

The toolkit presents a comprehensive road map that outlines critical steps and review gates, guiding stakeholders from initial planning through final implementation. The guidance emphasizes fundamental considerations of planning, governance and feasibility, acknowledging that successful digital identity management solutions must deliver tangible benefits and demonstrate sustainable financial planning.

Financial sustainability is paramount, requiring robust funding strategies not only for initial implementation but also for ongoing operational costs, maintenance and continuous improvement. The development of comprehensive assumptions and a detailed business plan represents a crucial component of the implementation process.

While this section provides a generic approach to Digital ID systems, Part III of the toolkit will dive into the specific technical aspects of an IOM software to be developed, focusing on the organization's particular use case for a Free Movement Zone in the context of migration. Despite the variations, the underlying technological principles remain consistent between the generic and IOM-specific implementations.

The toolkit acknowledges the significant variability in Digital ID implementation across different national and governmental contexts. To support countries in this complex endeavour, IOM offers specialized services focused on strategic planning and capacity-building, helping nations navigate the intricate process of developing digital identity systems.



2.1 GOVERNANCE AND GENERAL GUIDANCE

This section provides a comprehensive, sequential framework for planning and implementing a digital identity project, outlining the critical steps and strategic considerations essential to successful Digital ID development.

2.1.1 PROJECT SETUP

The initial phase of a Digital ID project requires strategic resource engagement and preliminary project planning, typically aligned with a government entity or executive office prior to establishing final governance structures. The primary objective is to create a foundational framework that can potentially evolve into a comprehensive digital identity initiative.

A dedicated project committee or working group is essential, comprising key stakeholders from various authorities and with a clear leadership structure and executive steering committee to facilitate critical decision-making processes. This multidisciplinary team will be responsible for guiding the project's strategic direction and ensuring comprehensive oversight.

The project's operational parameters will be defined by a comprehensive Project Charter that articulates the vision, objectives, decision-making protocols and fundamental project management procedures. This charter serves as the primary governance document, outlining specific project steps and critical decision gates required for successful implementation.

When requested, IOM can provide specialized support services to assist countries in navigating the complex process of Digital ID system development. The committee may also leverage external specialists from governmental or international organizations to conduct supporting research and provide technical expertise.

The Project Charter will ultimately establish a structured approach that ensures methodical progression from initial concept to full implementation, with clear governance mechanisms and strategic alignment.

2.1.2 ANALYSIS AND INFORMATION GATHERING

The initial planning and information gathering phase centres on comprehensively evaluating a country's digital infrastructure and population register sophistication. This digital maturity assessment represents a critical milestone in Digital ID project implementation, with the project's success directly correlating to the existing technological and administrative capabilities.

The evaluation encompasses a detailed analysis of technological infrastructure, institutional readiness and population registration systems. IOM supports this critical assessment through a specialized digital maturity toolkit, which provides a structured approach to infrastructure analysis.

A central focus of this evaluation is the examination of existing population registers, with particular emphasis on establishing identity uniqueness through robust identification mechanisms. Key assessment criteria include the presence of a comprehensive register containing a unique identifier, comprehensive biographic data and multiple biometric markers, including photographic and additional biometric information.

The assessment results will serve as a foundational discussion framework for determining the strategic approach to Digital ID implementation. By methodically evaluating digital infrastructure and registration systems, countries can develop a tailored, realistic road map for advancing their digital identity capabilities.

2.1.3 IDENTIFICATION OF STAKEHOLDERS AND OPERATING ENTITY

Following the initial infrastructure assessment, the potential stakeholders must be identified. This involves identifying entities with direct connectivity or those offering digital services that could potentially integrate with the Digital ID system. A strategic approach to stakeholder engagement includes conducting joint workshops and individual consultations to thoroughly understand the diverse requirements and prioritize Digital ID related services.

The assessment process will systematically evaluate existing digital government services, focusing on their current authentication mechanisms, identity management protocols and usage patterns. This analysis will result in a comprehensive application catalogue that documents the entire government service infrastructure, categorizing digital services by their functional characteristics and potential Digital ID integration opportunities.

The application and use case catalogue will serve as a critical planning document, providing detailed documentation of each entity's functional description, service characteristics and digital service landscape. This methodical documentation is mandatory for developing a strategic road map for Digital ID application services, ensuring a comprehensive and well-informed implementation approach.

By meticulously mapping stakeholder needs and existing digital service frameworks, governments can develop a targeted, efficient Digital ID strategy that aligns with institutional requirements and technological capabilities.

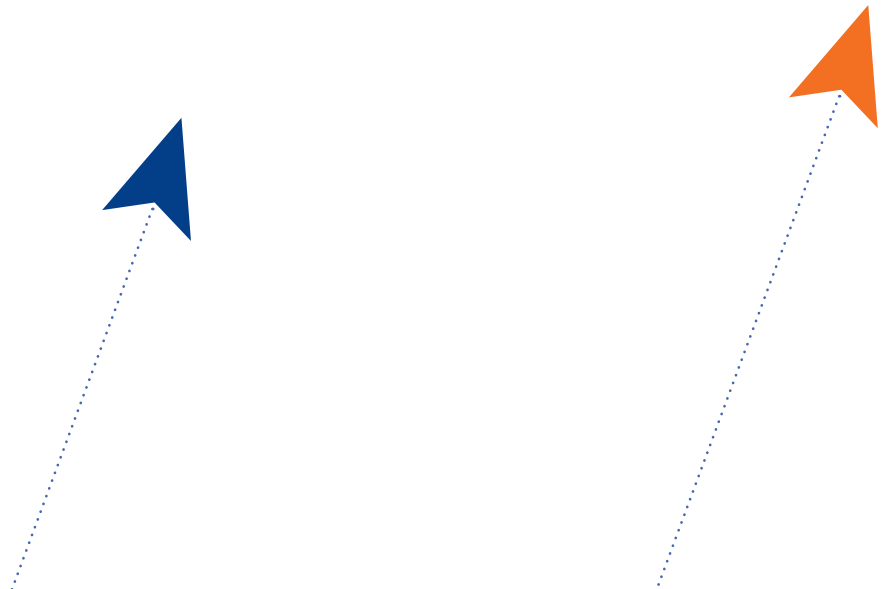
2.1.4 APPLICATION AND USE CASES

Based on the application and entity service catalogue, the next planning phase involves identifying high-maturity digital services with widespread usage. The recommended approach prioritizes these key applications while strategically initiating the Digital ID implementation with simpler, more manageable application profiles to ensure successful initial deployment.

The entire service catalogue will be transformed into a strategic application road map, incorporating a detailed time schedule that requires collaborative validation and agreement with service-providing entities. A critical consideration in this planning process is the necessary systems integration work required by each participating entity, which involves launching dedicated IT modification projects.

Each entity's integration effort will necessitate comprehensive IT system adaptation, including tendering procedures, system modifications and implementation timelines. These complex technical transitions must be carefully mapped and synchronized within the overall Digital ID implementation road map.

To ensure comprehensive and coordinated implementation, continuous planning sessions will be conducted. These collaborative meetings will facilitate detailed implementation planning, road map synchronization and ongoing stakeholder alignment, creating a dynamic and responsive approach to Digital ID system development.



2.1.5 LEGAL REQUIREMENTS

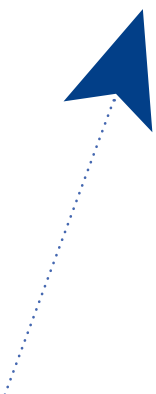
The legal requirements analysis represents a critical component of the Digital ID implementation strategy, directly aligned with the project's application road map. A comprehensive legal assessment must systematically evaluate existing digitalization laws and identify potential gaps requiring new legislative instruments, regulations or bylaws.

The analysis will determine which implementation components can proceed under current legal frameworks, and which necessitate new legislative development. A strategic approach focuses on initial use cases that align with existing legal provisions, potentially enabling parallel tracks of implementation and legislative expansion.

A key recommendation includes assessing KYC regulations across government-regulated private sectors such as banking, insurance and telecommunications. Early engagement with these regulatory frameworks can significantly expedite future Digital ID integration in private sector domains, recognizing that regulatory modifications consume substantial time and resources.

The legal assessment must also evaluate technical security audit requirements from local regulatory authorities. Doing so ensures comprehensive compliance and risk mitigation throughout the Digital ID implementation process.

The final implementation decision can only be rendered once the entire system is demonstrably compliant with current, valid local legal and regulatory standards. This meticulous approach ensures legal soundness, minimizes potential implementation risks and provides a robust foundation for Digital ID system development.



2.1.6 FINANCING AND BUSINESS PLAN

Together with other project development activities, a comprehensive financial model must be established to support the Digital ID implementation. The financial assessment will encompass comprehensive cost estimates, including system requirements, organizational staffing, physical infrastructure and both implementation and operational phases.

The business plan will develop a detailed five-year financial projection, distinctly categorizing (CAPEX for initial setup and OPEX for ongoing maintenance and system expansion. Initial financial modelling will focus on precise cost estimation, followed by a strategic evaluation of potential financing mechanisms.

Potential financing strategies may include international donor contributions, government budgetary allocations or cost-sharing arrangements among participating government entities. Ensuring a balanced cash flow fully supported by external financing sources is critical to the financial strategy.

An alternative implementation approach involves a concession model, where an external entity develops and operates the system before transferring ownership to the Government. Given that Digital ID systems typically do not generate direct revenue, such arrangements are most viable when integrated with complementary revenue-generating projects.

One promising approach is linking Digital ID implementation with travel document systems such as passport and identification card projects. This integration can provide a more financially attractive framework, especially for countries with significant document issuance volumes. The project can be structured so that the Digital ID component becomes a value-added element of a larger documentation system.

Regardless of the financing model, the contractual framework should prioritize open-source Digital ID software and include a comprehensive handover mechanism. This approach ensures government ownership and long-term sustainability of the digital identity infrastructure.

Each implementation will require a nuanced, case-specific financial assessment to determine the most appropriate financing and operational strategy.

2.2 TECHNICAL CONSIDERATIONS FOR DIGITAL IDENTITY MANAGEMENT

This section highlights technical considerations essential for the strategic planning and successful implementation of a Digital ID system.

2.2.1 EXISTING INFRASTRUCTURE AND GAP ANALYSIS

The analysis of digital maturity has already provided an initial indication of how a Digital ID could be implemented. The existing infrastructure analysis focuses on the detailed IT and network systems currently in place, to which the Digital ID system must be seamlessly integrated. At first glance, this does not directly concern other entities participating in the federated SSO. However, assessing whether all connected entities are using the same unique identifier is essential. If discrepancies exist, these entities will need to perform data migration and synchronization tasks to align unique identities, ensuring secure authentication.

The assessment should encompass all technical aspects of the existing identity management framework, identifying any potential gaps that need to be addressed. This exercise includes analysing the entire identity lifecycle and related registries to ensure a comprehensive understanding of the infrastructure and any necessary improvements.

2.2.2 DESIGN ARCHITECTURE AND DEVELOPMENT

The design and development of the proposed system architecture require a comprehensive analysis of the existing infrastructure. The Digital ID system must integrate with major national systems, leveraging existing data, technical interfaces and the capacity to handle the anticipated transaction volume. In addition to security and architectural considerations, careful planning for database and transaction capacity is essential.

A critical step in the development process is determining the implementation approach, that is, whether to adopt an open-source solution or a vendor-specific system. Open-source solutions offer the advantage of potential implementation by local system integrators, fostering job creation and knowledge transfer within the country. Alternatively, global IT integrators can be engaged for such implementations. Vendor-specific solutions, on the other hand, are typically provided by a limited number of identity management firms offering proprietary systems that are often reliable but closed-source.

Governments have adopted varying strategies: some initially implement proprietary solutions to achieve a quick launch and gain operational experience. During this phase, the responsible entity can build organizational capacity while benefiting from the vendor's managed approach, where not all aspects must be addressed simultaneously. At a later stage, governments may transition to open-source or in-house solutions to increase control and flexibility. Another approach involves the direct implementation of an open-source solution by a major IT integrator, followed by the gradual transfer of development, maintenance and operations to a government entity or local IT providers.

To select the most appropriate strategy, it is recommended to issue a Request for Information (RFI) to gather market insights and budgetary estimates. This evaluation will help assess the total cost of ownership for each option. Based on the RFI results, the strategy can be refined before issuing a formal tender for system implementation.

In addition to market options, the MOSIP project, initiated by the Institute of Information Technology in Bengaluru, promotes an open-source implementation of an identity management framework with a generic approach. The framework includes Inji, a mobile wallet for Digital ID and eSignet, a SSO solution.

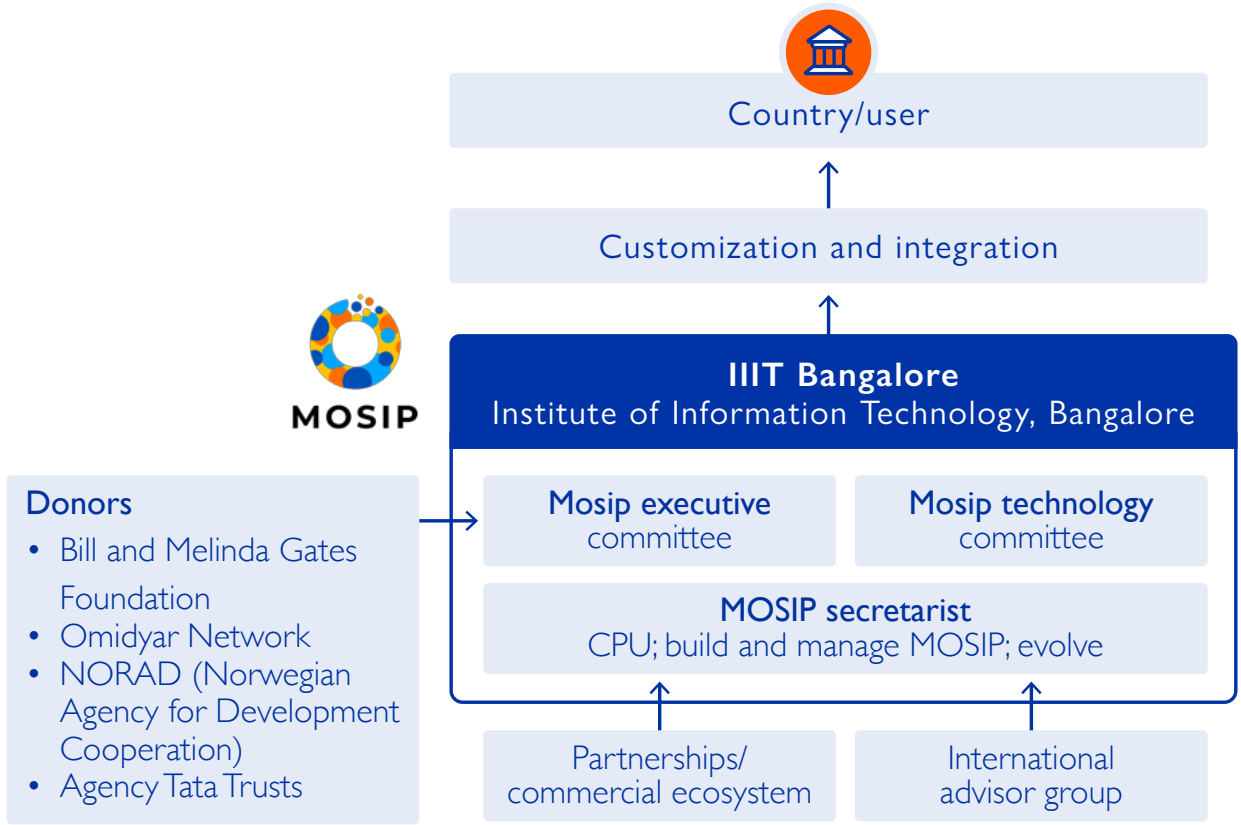
Key considerations for the IT system architecture:

- **Scalability by design:** Ensure the system can handle expected utilization and capacity.
- **Privacy and security by design:** Ensure data protection and privacy are built into the system.
- **Implementation approach:** Decide between an open-source, open-interfacing or single-vendor solution.

2.2.3 MOSIP PROJECT AS GENERIC EXAMPLE DESIGN

MOSIP is an initiative incubated at the Institute of Information Technology Bangalore (IIITB), aimed at developing an API-based foundational identity platform and supporting reference implementations. It enables countries to build their own identity management systems using MOSIP's source code, allowing them to gain independence from industry vendors. The initiative is funded by international donors such as Norad (Norwegian Agency for Development Cooperation), the Gates Foundation, Pratiksha Trust and Tata Trusts.

Figure 26. MOSIP



The Digital ID infrastructure is based on a back-end system linked to the population register or other national identity databases. A government customizes and configures MOSIP, deploys the identity solution in its data centres, and operates and maintains the system. While the objectives of identity systems across different counties may be similar, they may rely on proprietary technologies from specific vendors. MOSIP's framework integrates with population registers and includes modules for pre-registration, biometric registration, back-office identity checks and deduplication with biometric matchers. The approach allows countries to manage the core identity management system and freely choose suppliers, promoting competition and reducing vendor lock-in.

MOSIP works on various platforms and supports certified devices for biometric capture globally. In addition to the foundational identity system, MOSIP

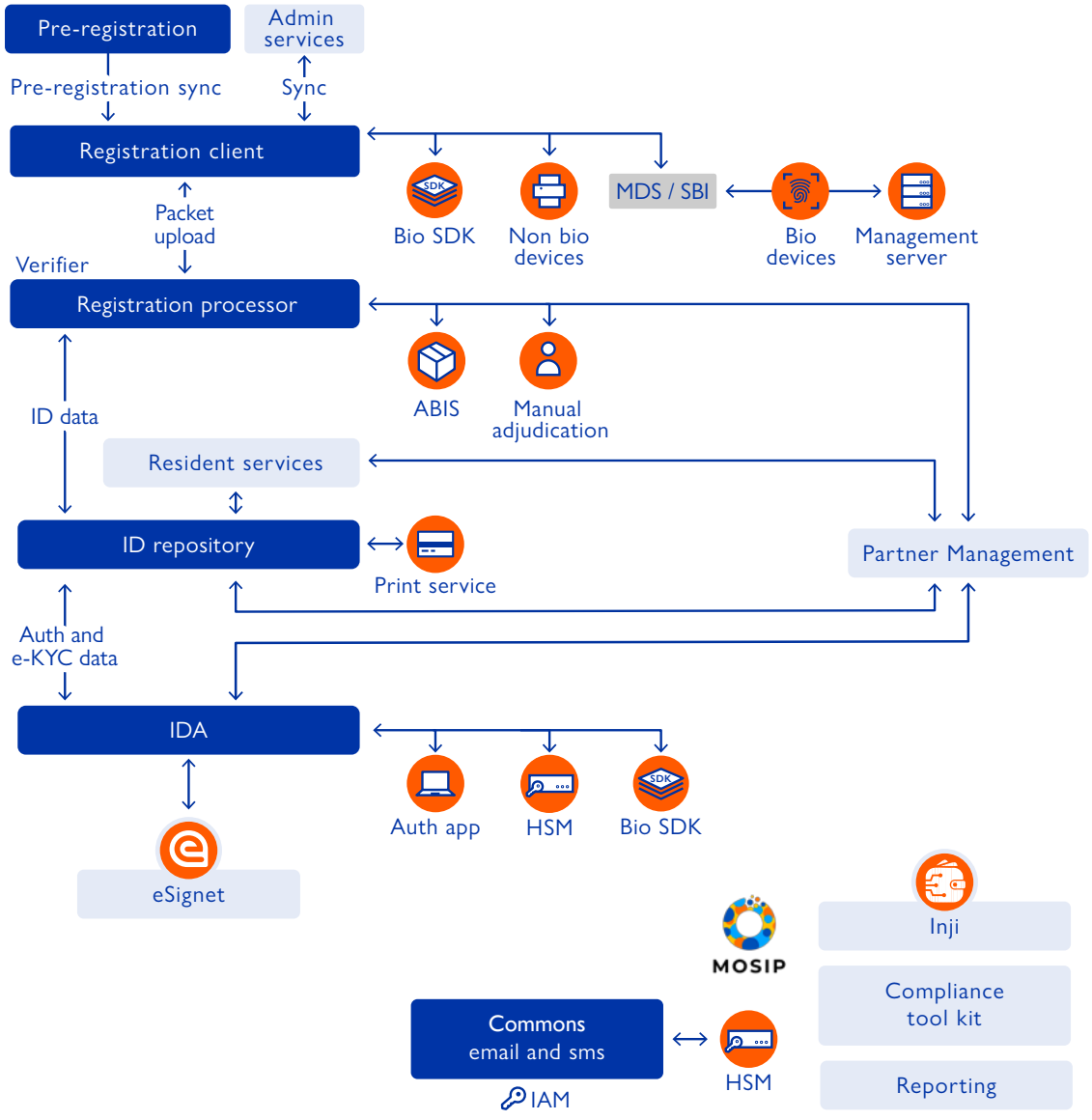
also offers additional reference implementations and modules for data exchange for verification of IDs. These include Inji, a credentialing stack and digital identity wallet that facilitates the secure issuance, digitalization, storage, and verification of Verifiable Credentials (VCs), as well as eSignet, and single sign-on application.

As a technology stack, MOSIP uses standard Java, related APIs, and Angular for the front end, all widely used for web-based applications. To avoid proprietary licenses, MOSIP uses PostgreSQL for its database. This open-source approach ensures flexibility and extensibility as important advantages but also requires careful customization and ongoing maintenance to meet evolving needs.

The Digital ID system is part of a larger government identity management ecosystem, connected to the civil registration database, which manages life events and may integrate with other systems such as immigration databases for legal residents.

Figure 27 outlines the Digital ID management infrastructure based on MOSIP. Government infrastructure typically grows over time, requiring customized integration and potentially replacing old systems. The availability of IT infrastructure for resident registration and communication, along with the high number of enrolled residents, remains a challenge and is key to the country's digital maturity for successful Digital ID implementation.

Figure 27. MOSIP's infrastructure overview



Source: MOSIP.

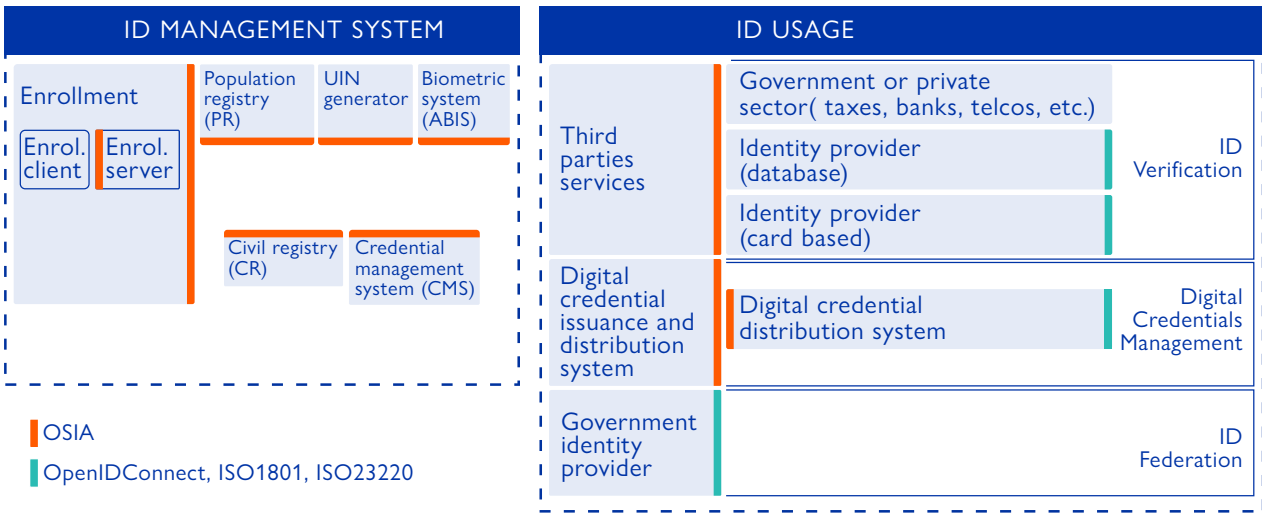
2.2.4 INTEROPERABILITY FRAMEWORK OSIA (ITU-T X.1281)

The OSIA specification has been recognized in 2024 as an international standard by the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T). The specification of the interoperability framework is listed as ITU-T Recommendation ITU-T X.1281 - APIs for interoperability of identity management systems.

The framework enabling Open and Transparent Identity Systems OSIA, supports government-industry collaboration to establish open national ID systems and address interoperability challenges through a defined approach:

- OSIA formalizes the scope and functions of key identity system building blocks.
- Standardizing Interfaces and Data Exchange – OSIA develops standardized interfaces and a universal data dictionary, enabling seamless interactions between components while allowing governments to customize processes according to local laws.

Figure 28. OSIA framework interface structure



Source: www.osia.io.

OSIA delivers transformative benefits across the identity ecosystem by ensuring interoperability, fostering competition and enhancing service delivery.

- **Enabling market innovation:** OSIA levels the playing field for vendors by providing standardized interfaces without favoring specific technologies. This approach encourages competition and supports local suppliers and SMEs.
- **Eliminating vendor lock-in:** Governments gain flexibility to mix and match components from different suppliers or extend legacy solutions without compatibility concerns. This autonomy empowers governments to develop sovereign identity systems aligned with national priorities.
- **Enabling identity as a service:** OSIA facilitates the deployment of Digital ID solutions, improving access to eGovernment services and trusted online transactions. By linking sovereign identity systems with digital identity solutions, OSIA strengthens fraud prevention and enhances the security of ID verification processes.

OSIA and the Digital ID landscape

OSIA's interoperability framework extends to identity verification and digital credential management. The OSIA Relying Party API allows third-party services to validate citizen ID attributes, streamlining processes like telecom enrolment and banking services. OSIA also integrates with ISO Digital Credential Management and OpenID Connect Federation.

2.2.5 SYSTEM OPERATION

The operation of the system must incorporate a dedicated technical and operational maintenance team, along with a user help desk. The size of the organization will depend on the system's complexity during the initial implementation phase. Key areas of operation should include IT and application management, hardware support and maintenance, a user help desk and a separate team for IT security and service quality monitoring. The organizational structure required can initially resemble a small IT company, scaling up to a 24/7 IT service organization as system usage grows.

The IT hosting operation must account for robust physical security measures to protect access to IT systems and incorporate architecture designed for disaster recovery and business continuity. This may involve setting up a backup site capable of taking over IT services in case of a primary site failure. The data centre infrastructure could be government-owned or housed in private colocation facilities, provided the Government retains full control. Regardless of the ownership model, the infrastructure should comply with at least Tier 3 standards as defined by globally recognized data centre classifications. A Tier 3 data center ensures redundancy in critical systems such as power supply and cooling to mitigate operational risks. The Digital ID infrastructure should be regarded as critical national infrastructure, requiring high levels of security and availability. Before selecting a hosting location, the data centre infrastructure should be assessed and certified according to international standards, with preference given to certified facilities meeting the required standards.

In addition to operational resources and infrastructure, IT security is a cornerstone of trust, particularly for systems involving Public Key Infrastructure (PKI). To ensure robust IT security, it is recommended to implement and maintain an ISO 27001-certified Information Security Management System. This certification ensures the implementation of security controls, risk assessments, and effective incident management processes. The ISO 27001 framework requires regular audits, including annual partial audits and full audits every three years, to maintain compliance and uphold system integrity.

2.3 DIGITAL IDENTITY USE CASE PLANNING

When implementing a Digital ID system, selecting a key use case for implementation is crucial. In many cases, various government entities have already implemented digital services or are in the process of doing so. These digital applications could serve purposes such as education, document applications, tax declarations or other administrative processes.

A recommended initial application is a federated SSO system, enabling users to log in and access multiple government services seamlessly. To determine the best starting point, it is essential to evaluate which government service or entity's digital application is most frequently used. Once the Digital ID system is integrated with this use case, it can serve as a model to demonstrate its benefits and encourage adoption among users.

Over time, using a Digital ID to access government services should become mandatory. As the user base grows and more people enrol in the Digital ID system, additional applications and services can be integrated, further expanding its utility and value.

2.3.1 IMPLEMENTATION ROAD MAP

With the initial use case and overall planning in place, an implementation road map should be developed. This road map can span a period of three to five years and should be reviewed annually to ensure the feasibility and effectiveness of the applications integrated with the Digital ID. Potential use cases should be identified based on the country's broader digitalization initiatives.

Once the initial key use case is operational, the road map can outline the onboarding of additional services. As a priority, it is recommended to integrate a certain number of SSO government portals to maximize the presence of the Digital ID app across citizens' and residents' digital devices.

Recognizing that public acceptance of new use cases added to the Digital ID app may take time is important, as people adjust to using the system. To support this transition, a sustained marketing campaign should be implemented to raise awareness and promote Digital ID usage.

Over time, the road map should include essential services with broad public appeal, such as education enrolment, retirement services or tax applications, as these areas engage large segments of the population. The overarching goal of the road map is to drive widespread adoption of the Digital ID across the application landscape.

Additionally, semi-government and regulated sectors such as banking, insurance and telecommunications provide valuable opportunities for use case expansion. However, when integrating such applications, careful consideration must be given to the legal implications, regulatory requirements and liability concerns involving third-party entities outside the Government's domain.

Ultimately, the Digital ID application road map must be tailored to the country's specific infrastructure, regulatory environment and current stage of digital development.

2.3.2 STRATEGIC PLANNING

The planning for use cases should align with the broader strategy for the digitalization of government infrastructure. A long-term strategic plan, covering 10 to 20 years with periodic reviews, will support overall infrastructure development as well as specific Digital ID support for new services and applications. With the initial use case and overall planning in place, an implementation road map should be created. The Digital ID road map, aligned with the strategic plan, should span blocks of three to five years, with periodic reviews. The long-term strategy will provide guidance on the general direction, while the Digital ID implementation and use case road map will focus on direct execution.

2.4 COMPLIANCE CONSIDERATION

This section offers a principal overview of compliance and regulatory considerations. Throughout the planning and implementation of a Digital ID system, regular assessments of compliance with local and international standards are essential. This ensures adherence to applicable regulations and enables timely adjustments to implementation efforts to maintain compliance at all stages.

Digital ID and identity management systems handle sensitive personal information and facilitate access to government services, encompassing the entire population. As such, ensuring compliance with data protection and security standards is critical to safeguarding privacy and maintaining trust.

IOM provides valuable guidance through its Data Protection Manual. To align with international best practices, compliance with frameworks such as the General Data Protection Regulation[19] and other relevant local data protection regulations should also be incorporated.

2.4.1 DATA PROTECTION AND PRIVACY OF PERSONAL DATA

Data protection and privacy regulations are fundamental pillars of Digital ID systems and the digital services they support. The planning and implementation phases must be thoroughly evaluated against applicable local data protection policies and standards. This evaluation includes ensuring compliance with user consent policies, legal documentation and data handling practices, as well as implementing robust security measures to prevent unauthorized data access, breaches or leaks.

It is strongly recommended that the local data protection authority or a dedicated Data Protection Officer be involved in conducting independent and ongoing assessments during the planning, implementation and operational phases. Additionally, a comprehensive set of monitoring procedures should be established to ensure continuous compliance and address emerging risks.

As a basic principle, any personal data collected shall only be used for the purpose they have been collected for and with full consent from the user at the time of usage of personal data or at the time of collection.

2.4.2 INTERNATIONAL REGULATIONS AND HUMAN RIGHTS CONSIDERATIONS

Compliance considerations must encompass adherence to international regulations regarding anti-corruption and ethical standards. The use of biometric information should strictly align with international guidelines, ensuring that biometric data collected for identification purposes is securely protected and used solely for user authentication within the Digital ID system. The use of biometric data must not extend beyond the Digital ID system, and it must always be obtained with the user's explicit consent.

The Digital ID system must prioritize the protection of users and their data, incorporating robust safeguards to uphold privacy and security.

Additionally, the system must guarantee equal treatment for all individuals within the country, irrespective of ethnic origin or religion. Continuously assessing the system's alignment with human rights principles and ensuring compliance with standards promoting fairness and equality is essential.

19 For more information on General Data Protection Regulation, see here.

2.5 NON-COMPLIANCE CONSIDERATIONS

Non-compliance with laws and regulations, such as data protection or incidents of data breaches, can have serious consequences for a Digital ID system. These consequences include legal and financial repercussions as well as significant damage to public trust. Trust in the system's security and reliability is crucial for its success. A loss of trust can lead to widespread rejection, making the system ineffective and unused.

To mitigate these risks, ongoing assessments of compliance and risk factors are essential. Regular risk assessments and the implementation of appropriate risk management measures are critical to maintaining compliance and protecting the system.

If international funding or donations are involved, non-compliance could result in the suspension or termination of financial support, jeopardizing the project's sustainability and success.

Implementing internationally recognized Quality and Security Management systems is recommended. These systems include:

- Quality Management in accordance with ISO 9001;[20]
- Information Security Management System in accordance with ISO 27001;[21]
- Business Continuity in accordance with ISO 22301;[22]
- International IT Service Management Standard ISO 20000;[23]
- Environmental Management Systems ISO 14001.[24]

The implementation of international standards for quality and services provides strong resilience against non-compliance. These standards are management systems that must be aligned with the service, organization and systems, and include risk management, continuous review, audit and improvement processes.

2.5.1 SPECIFIC NON-COMPLIANCE CONSIDERATIONS

Quality

Non-compliance with the quality of service or availability is a warning sign indicating problems in technical systems or processes. If identified and mitigated quickly, the overall quality can be improved. In such cases, corrective measures or changes can help eliminate the root cause of non-compliance and meet citizens' service expectations efficiently.

Cost

Non-compliance can imply additional costs, such as loss of service transactions for government entities, help desk calls, or required communication with citizens. However, with a proper response to non-compliance, additional costs can be avoided.

20 ISO, ISO 9001:2015 Quality management systems – Requirements (ISO, 2015).

21 ISO, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO, 2022).

22 ISO, ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements (ISO, 2019).

23 ISO, ISO/IEC 20000-1:2018 Information technology –Service management Part 1: Service management system requirements, 3rd edition (ISO, 2018, reviewed and confirmed in 2023).

24 ISO, ISO 14001:2015 Environmental management systems – Requirements with guidance for use (ISO, 2015).

Customer satisfaction

Non-compliance can lead to customer dissatisfaction and complaints, which, if escalated in social or public media, can cause additional damage to trust in the Digital ID system or rejection by users. Customer complaints shall be responded to in time to prevent escalation and provide input for continuous improvement. Citizens are the end users, and if Digital ID services are used frequently and easily, customer satisfaction will have a positive impact on the government entities offering the service.

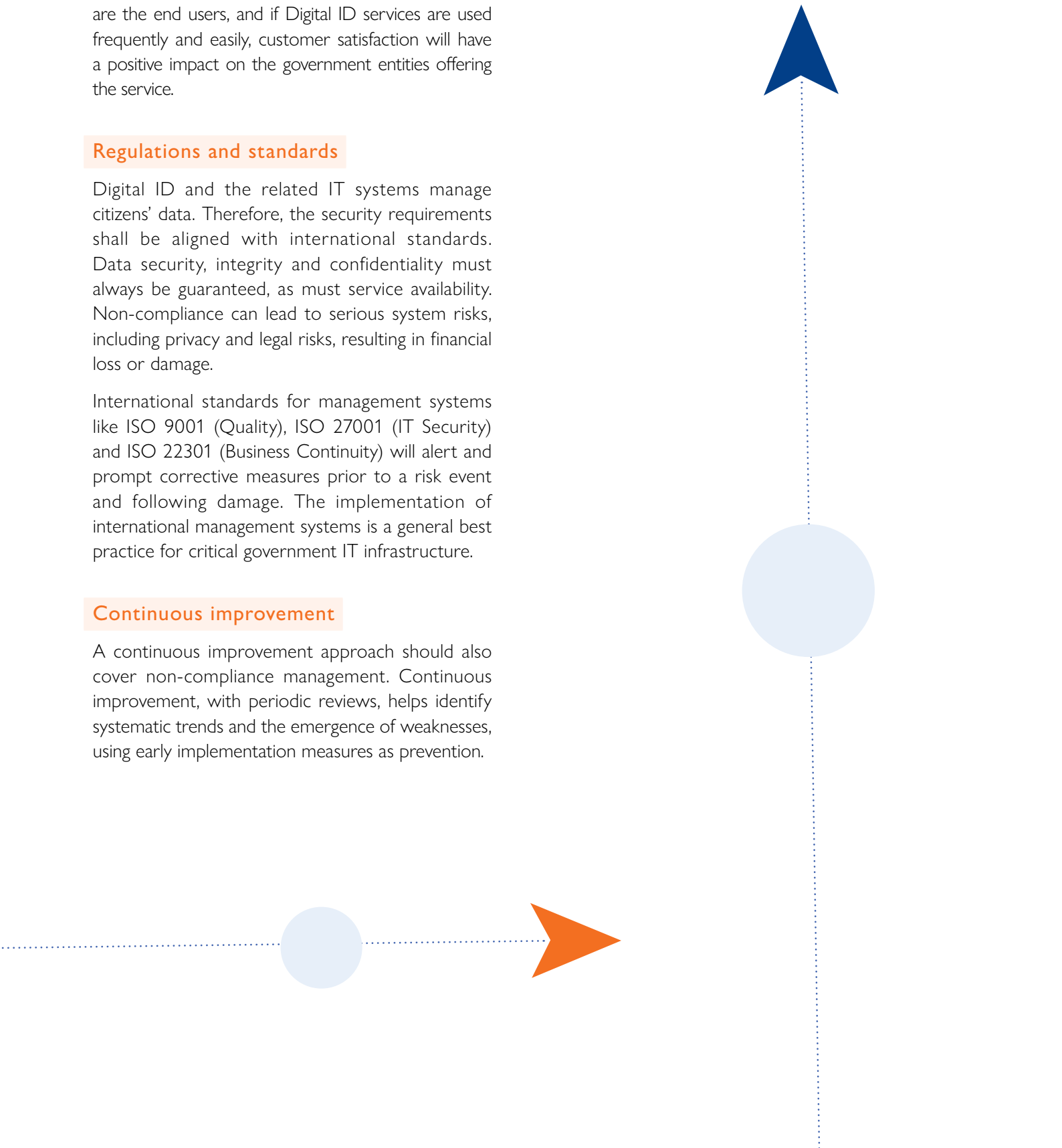
Regulations and standards

Digital ID and the related IT systems manage citizens' data. Therefore, the security requirements shall be aligned with international standards. Data security, integrity and confidentiality must always be guaranteed, as must service availability. Non-compliance can lead to serious system risks, including privacy and legal risks, resulting in financial loss or damage.

International standards for management systems like ISO 9001 (Quality), ISO 27001 (IT Security) and ISO 22301 (Business Continuity) will alert and prompt corrective measures prior to a risk event and following damage. The implementation of international management systems is a general best practice for critical government IT infrastructure.

Continuous improvement

A continuous improvement approach should also cover non-compliance management. Continuous improvement, with periodic reviews, helps identify systematic trends and the emergence of weaknesses, using early implementation measures as prevention.



2.6 COMPLIANCE RISKS MANAGEMENT AND MITIGATION

Risk mitigation and preventive actions are well-established practices for identifying and addressing potential non-compliance risks. To ensure effective risk identification and management, the implementing organization should establish a dedicated quality and risk management function. This team would be responsible for continuously assessing risks and recommending proactive mitigation strategies to address them before they materialize.

Risk and compliance management should be regarded as a preventive approach, distinct from incident response, which deals with risks after they have occurred. Compliance risks can arise from various sources, such as corruption during procurement processes, data security breaches or potential cyberattacks. The primary goal of risk management is to identify all potential risks, assess their likelihood and impact, and develop customized mitigation plans to prevent and address each risk proactively.

Recommended measures for effective risk management include:

a. Conducting Compliance Assessments: regular compliance assessments can help organizations identify areas of non-compliance and formulate plans to address gaps effectively.

b. Quality Assessments and Reviews: to measure customer satisfaction.

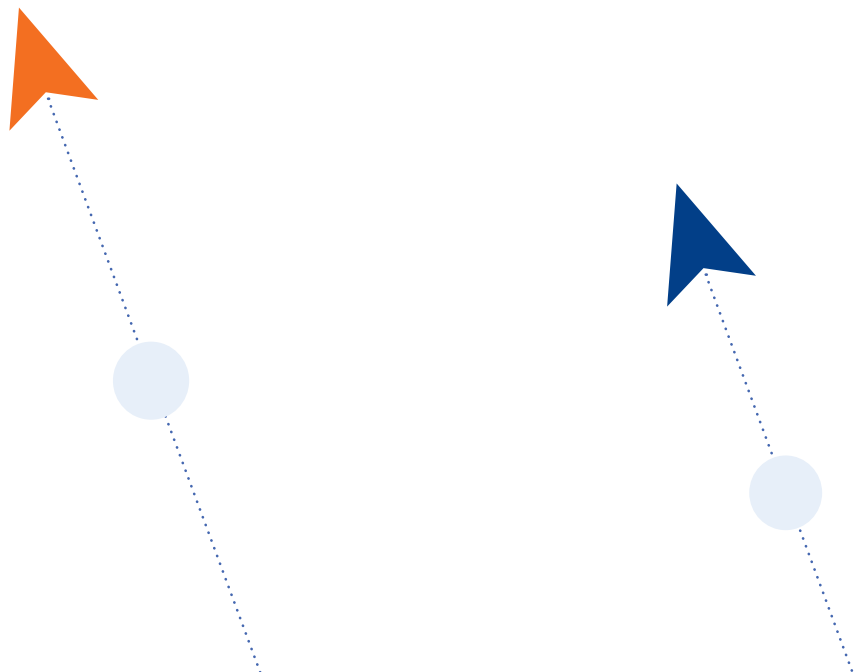
c. Continuous Risk Assessments: to identify any risks with substantial impact. A risk management policy and process should be implemented.

d. Implementing Security Controls: establishing robust security measures is essential to safeguard personal data, payment information and other sensitive assets, while managing cybersecurity risks.

e. Continuous Improvement: to identify potential weaknesses and implement measures to improve the system and related services.

f. Employee Training: providing employees with comprehensive training on compliance requirements and best practices for managing digital identities is critical to fostering a culture of awareness and adherence.

By incorporating these measures into the risk management process, organizations can enhance their preparedness and ensure compliance, minimizing potential risks and their associated consequences.



2.7 SUMMARY AND CONCLUSION

In conclusion, implementing a Digital ID system represents a significant milestone in advancing digital government services. This process requires meticulous planning, thorough assessments and strategic execution to avoid unnecessary setbacks and inefficiencies. The following key areas are critical for successful implementation:

a. **Assessment of Digital Readiness:** Evaluate the population registry, basic digital infrastructure, and identify potential enhancements to ensure readiness for the Digital ID system.

b. **Project Preparation and Legislative Framework:** Establish a clear project setup and develop a robust legislative framework to support the Digital ID system and its associated services.

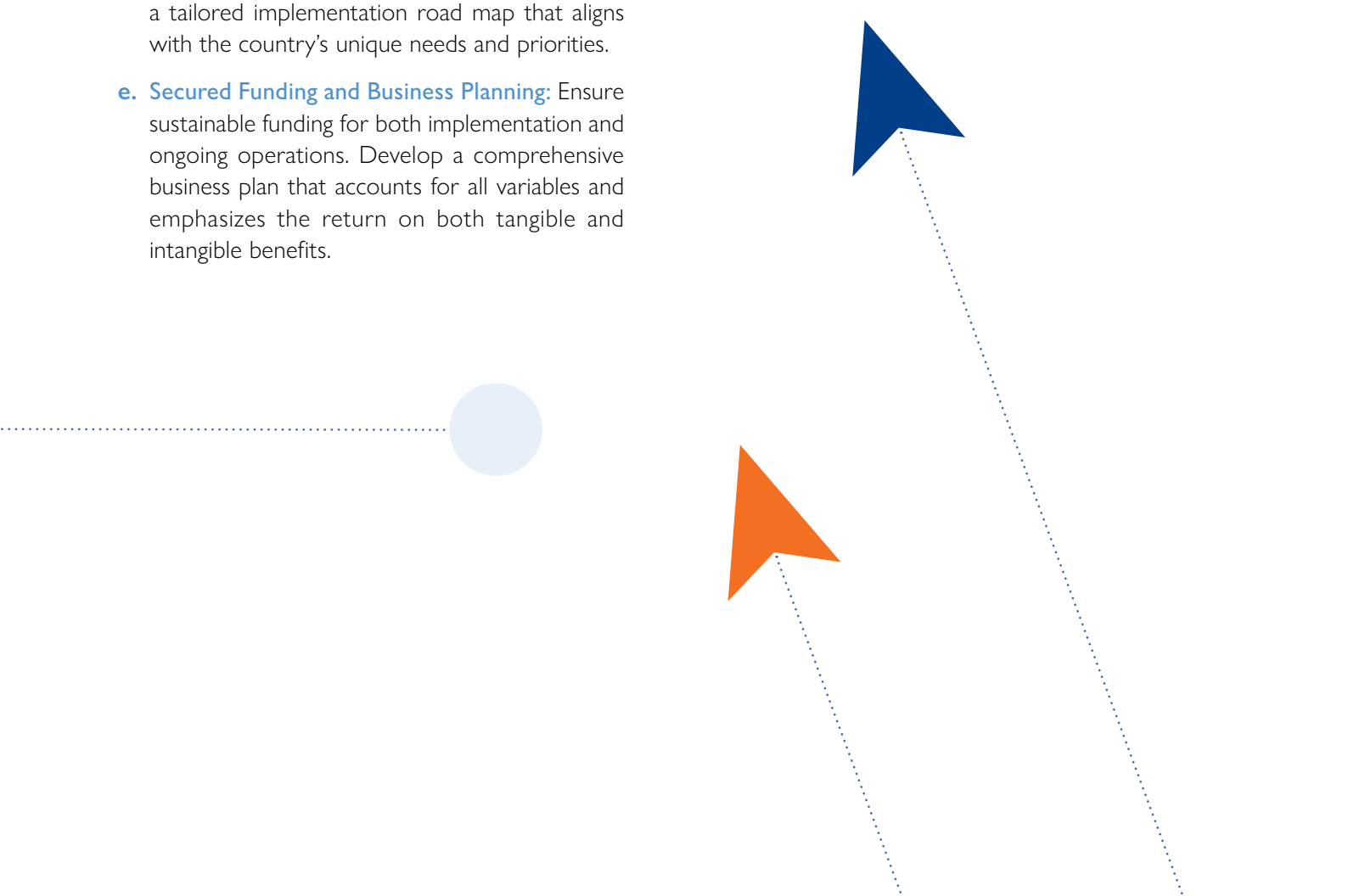
c. **Selection or Establishment of a Managing Entity:** Identify the most suitable existing entity or establish a dedicated organization to oversee the implementation and management of the Digital ID system.

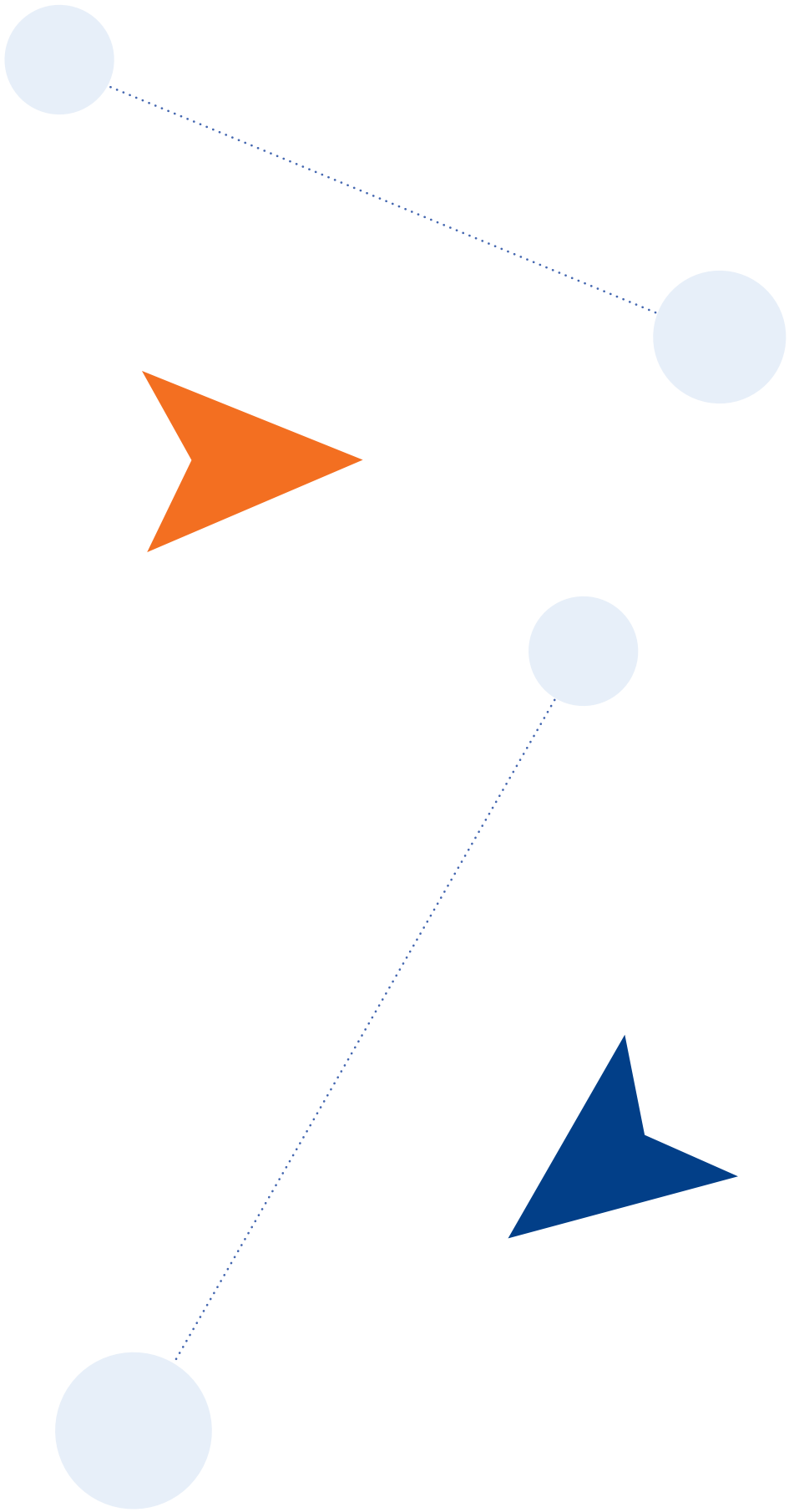
d. **Careful Selection of Use Cases:** Identify initial use cases and define key success factors. Develop a tailored implementation road map that aligns with the country's unique needs and priorities.

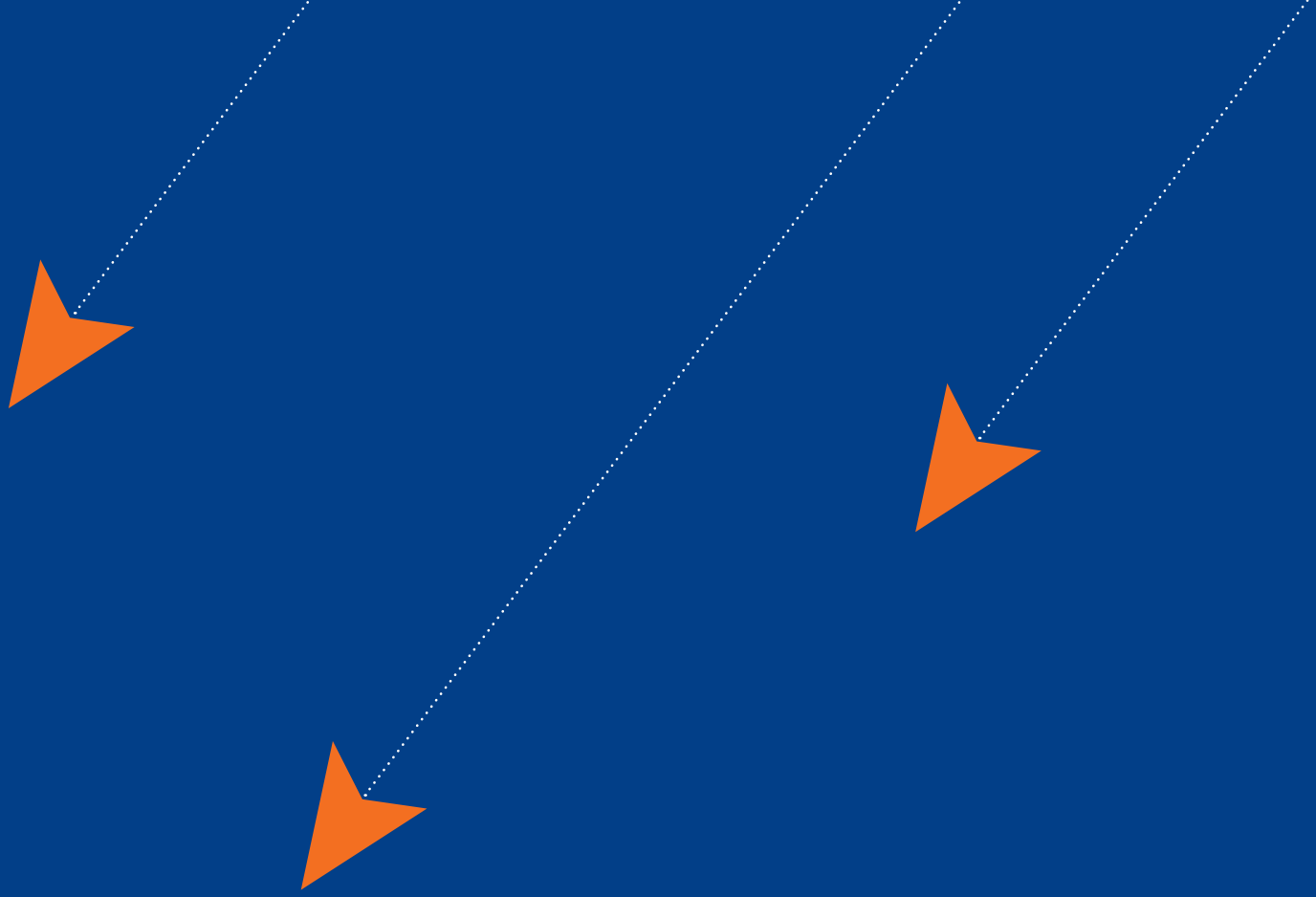
e. **Secured Funding and Business Planning:** Ensure sustainable funding for both implementation and ongoing operations. Develop a comprehensive business plan that accounts for all variables and emphasizes the return on both tangible and intangible benefits.

The procurement for systems and services shall follow the local regulation and best practice for governments. *ICAO's Best Practices for Acquisition of MRTD Goods and Services* provides an outline of the best practice for Machine readable travel documents. The methodology of the best practice could be transferred to the purchase of goods and services for Digital ID.

f. **The implementation of international management system standards,** for example ISO 9001 and ISO 27001, will help to prevent non-compliance risks and provide procedures for continuous audit, review and improvement.







PART 3

IOM Use-Case for Digital Identity

Part 3: IOM Use Case for Digital Identity

Part 3 of this toolkit presents a practical use case example in a migration context where IOM is involved. The objective of this example is to demonstrate how Digital Identity can facilitate safe and efficient pathways for movement within a free movement zone. The use case highlights the implementation of Digital ID solutions accessible via mobile phones while also accommodating alternative formats, such as QR codes on paper and various types of contactless smart cards. This inclusive approach ensures that all migrants, regardless of their access to advanced digital infrastructure, can benefit from the system, aligning with the available local and individual resources.

3.1 INTRODUCTION TO THE USE CASE: BORDER CROSSING IN A FREE MOVEMENT ZONE (FMZ)

The chapter provides an introduction and scope of the IOM example use case.

- Basic overview
- Key focus
- Usage of documents and Digital ID for the specific use case
- Based on bilateral agreement

3.2 KEY CONSIDERATIONS

The chapter explains the basic considerations of the use case.

- Objective
- Limitations
- Target group
- Documents for FMZ travelling
- Identity management
- Border control entry/exit

3.3 IOM USE CASE IMPLEMENTATION GUIDANCE ON CAPACITY-BUILDING

The chapter provides guidance through a project setup to implement the IOM use case.

- Assessment
- Planning
- Bilateral agreement
- Implementation
- Operation

3.4 APPLICATION OF THE DIGITAL IDENTITY TECHNOLOGIES

The chapter explains the used technology for the FMZ Digital ID system.

- General system description and components
- Key considerations
- Guidance for implementation in a Free Movement Zone (FMZ)
- Credential types and their handling

3.5 QUALITY AND SYSTEM PERFORMANCE

The chapter explains implementation and review of quality indicators.

- KPI definition
- Technical quality
- Data privacy and security

3.1 INTRODUCTION TO THE USE CASE: BORDER CROSSING IN A FREE MOVEMENT ZONE

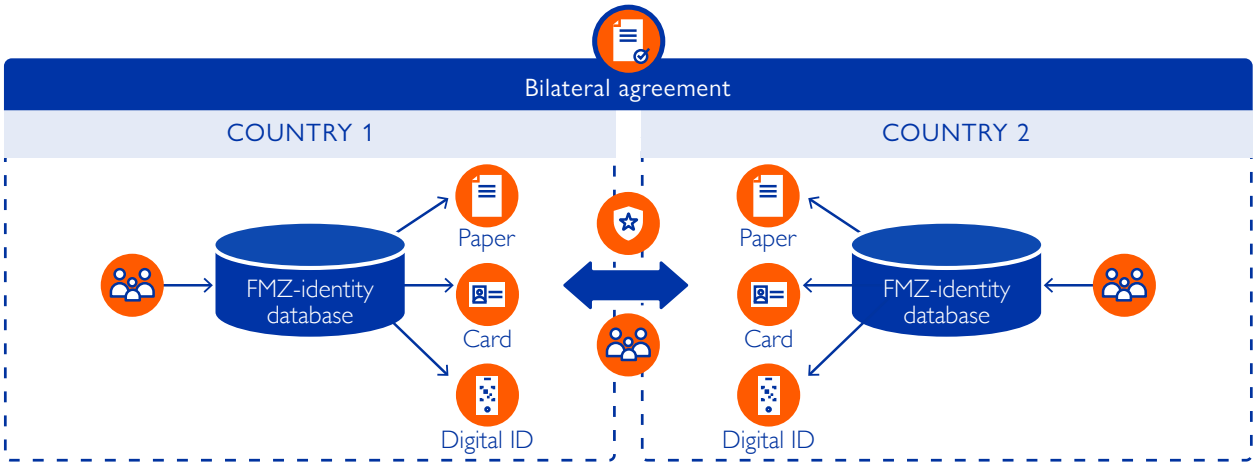
The use case for frequent border crossings pertains to borders where individuals regularly cross and return, often multiple times a day, for purposes such as trade, education or personal and family matters. Standard immigration procedures can significantly delay these crossings, and many individuals may lack ICAO-compliant travel documents. However, even in the absence of international travel documents, it is essential to ensure that all individuals crossing the border meet eligibility requirements, fulfil crossing criteria and have their crossings accurately recorded.

The implementation of a Digital Identity system offers a solution by providing a derived travel authorization specific to designated border points. This authorization is based on predefined criteria that are easily verified, eliminating the need for traditional immigration procedures or extensive pre-clearance processes. The IOM use case focuses on leveraging a digital credential and Digital ID system to support individuals within a designated Free Movement Zone (FMZ), ensuring appropriate levels of control at border-crossing points. This approach is not intended to represent the full-scale implementation of a national Digital ID system but is specifically tailored to address the security and operational requirements of limited FMZs.

The Digital ID system employed in this use case utilizes the same foundational technology as a national Digital ID system but adapts it with a simplified, use-case-specific information base. The technical design aims to maximize security while minimizing costs associated with credentials, infrastructure and implementation.

Each participating country manages or provides access to a database containing the identities of individuals eligible to cross the border under bilateral agreements. This database may connect to a civil registry or hold locally captured data solely for the purpose of issuing the Digital ID for the free movement pass. Regardless of the approach, this database serves as the authoritative source of identity and includes additional information confirming the individual's eligibility to cross the border under the terms of the agreement. This streamlined system ensures secure, efficient and cost-effective border management in designated zones.

Figure 29. IOM's Digital ID use case



3.2 KEY CONSIDERATIONS

The IOM Digital ID migration use case assumes a scenario involving two neighbouring countries with a shared border, where specific citizens from both sides frequently cross the border, often multiple times a day. These crossings are essential for facilitating trade, maintaining family connections, enabling education and promoting overall economic and social development.

In this context, the two countries agree to establish a designated FMZ governed by a clear policy framework. This zone is not intended for unrestricted movement but requires specific border control procedures to ensure that only eligible citizens can cross, thereby preventing irregular migration and minimizing criminal trafficking activities.

Under the bilateral agreement, both countries issue dedicated digital identity credentials to their eligible citizens. These credentials serve as the primary means of identification for border crossings within the FMZ. This use case focuses on rural or remote areas where standard immigration border controls are either impractical or non-existent. While these border crossings may be located near control points for international travellers, they are more commonly found in less developed areas without standard infrastructure.

In regions where citizens from both countries regularly cross the border, the absence of proper control mechanisms often leads to irregular and unregulated migration, accompanied by potential negative consequences such as trafficking and other criminal activities. Additionally, the technical infrastructure in these areas is often limited, and many eligible FMZ travellers may have limited familiarity with formal travel procedures. The challenge is to implement a system that provides an adequate level of security and control in such environments, while ensuring inclusive and safe migration for eligible citizens.

The IOM use case proposes a solution that uses digital identity and digital credentials to establish a secure and controlled border-crossing process within the FMZ. This approach ensures compliance with the bilateral agreement, facilitates safe and efficient movement for the target population and mitigates risks associated with unregulated migration and illegal activity. By addressing the unique needs of rural and remote border areas, the use case demonstrates how digital identity solutions can enhance security and promote lawful migration while fostering social and economic development.

IOM's use case limitations

The IOM use case and this document focus exclusively on the identification documentation and entry/exit procedures necessary to facilitate border crossings within a designated FMZ. It does not address the broader economic, social or political considerations associated with establishing such a zone. The use case is limited to outlining a technical system that uses digital credentials and Digital ID to enable and support secure and efficient movement across the border.

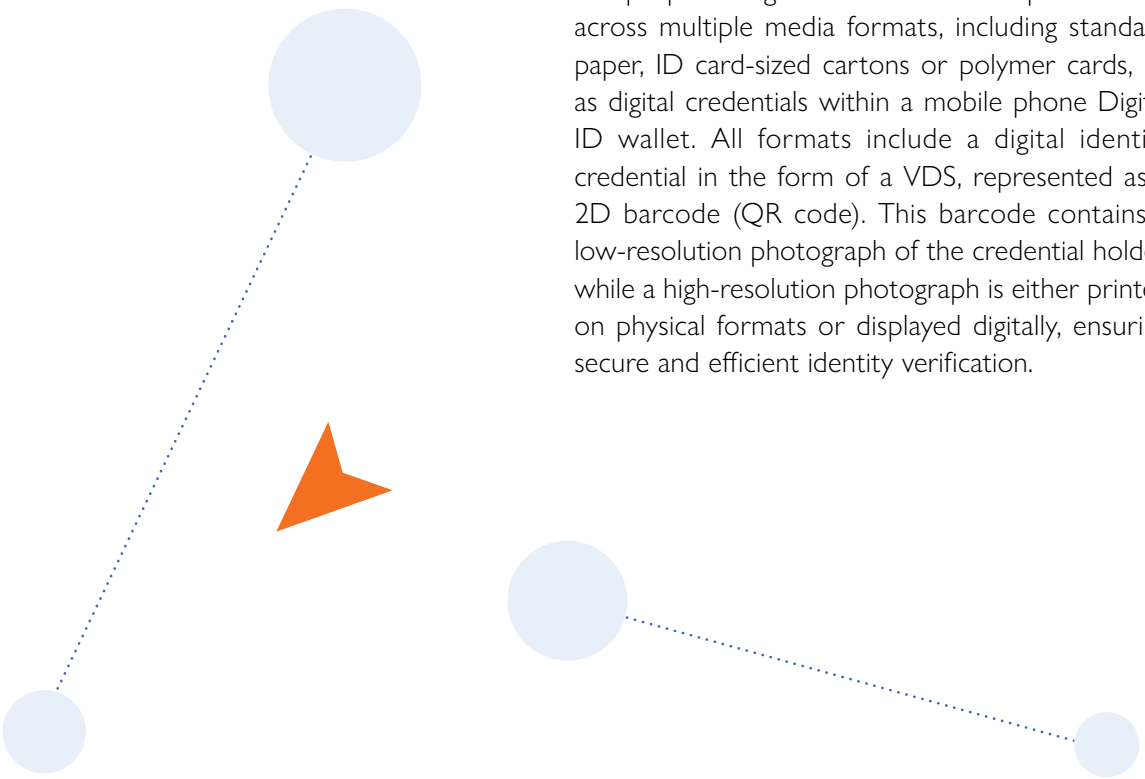
The main motivations and strategic rationale behind the creation of the FMZ fall outside the scope of this toolkit. Instead, the document focusses on the requirements for establishing an identity and digital credential policy between the participating countries, specifically for the purpose of travel facilitation within the FMZ.

Target group

The IOM use case targets citizens of all ages from both participating countries who are deemed eligible under the policy outlined in the bilateral agreement. The streamlined entry and exit procedures at border control points are exclusively available to these eligible citizens within the designated FMZ.

Travellers who are not registered or eligible under the FMZ agreement, such as tourists or business travellers, are outside the scope of this use case. These individuals must use standard border control points and comply with standard immigration procedures, including using ICAO-compliant international travel documents.

The participating countries jointly define the FMZ eligibility criteria, and eligible citizens are issued an FMZ-specific travel credential. This credential is intended solely to facilitate movement within the designated FMZ and for the purposes outlined in the bilateral agreement.



Documents for (FMZ) travelling

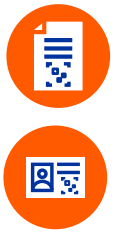
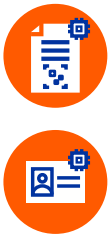
Not all individuals possess standard ICAO-compliant travel passports for international travel, and some may be unable to obtain them for various reasons. The proposed use case addresses this gap by introducing a streamlined border control process specifically for FMZ-eligible travellers. While the process eases crossing requirements, it maintains essential controls by registering entries and exits at designated FMZ border crossing points to monitor and manage movements effectively.[25]

To facilitate this process, the IOM use case recommends the use of digital identity credentials. These credentials can be issued in various formats and support a range of verification scenarios with differing security levels, from manual face verification to fully automated facial recognition systems. The specific types of documents to be issued and accepted are determined by the participating countries as part of their bilateral agreements and policies. The IOM use case serves to illustrate the different implementation options that are available.

The proposed digital credentials can be personalized across multiple media formats, including standard paper, ID card-sized cartons or polymer cards, or as digital credentials within a mobile phone Digital ID wallet. All formats include a digital identity credential in the form of a VDS, represented as a 2D barcode (QR code). This barcode contains a low-resolution photograph of the credential holder, while a high-resolution photograph is either printed on physical formats or displayed digitally, ensuring secure and efficient identity verification.

25 IOM has a *Free Movement Zones Guide* that can provide more information on the topic. The guide includes definitions of FMZ, reasons for establishing FMZs, examples of FMZ initiatives and guidelines on border management and credential design for FMZ travels.

Figure 30. IOM's Digital ID use case document types

DOCUMENT	PHYSICAL DOCUMENT	DIGITAL COMPONENT	BINDING OF DIGITAL CREDENTIAL
	Physical ID-card size carton/polymer card with optional security features or paper document with or without additional security features.	Digital identity credentials as VDS personalized as 2D barcode (QR code) with low-resolution photo of the bearer in the QR code together with a high-resolution printed photo.	The digital credential is not directly bound to the physical medium. The physical document can be secured using traditional security features to prevent copying and counterfeiting, while the digital credential itself ensures robust digital security. Other methods that link digital credentials to physical documents, which are proprietary in nature, fall outside the scope of this use case and are not addressed here.
	Lightweight secure chip (referred as Type-1) embedded in a secure label applied to a paper document or inside an ID-card size carton/polymer card.	Digital identity credentials as VDS personalized as 2D barcode (QR code) with low-resolution photo of the bearer in the QR code together with a high-resolution printed photo.	The chip is securely integrated with the digital credential, ensuring protection against reproduction or duplication. Additionally, the card or paper can be enhanced with traditional security features if necessary.
	An RFID SmartChip with ID-grade security (referred to as a Type-2 token in the IOM use case) embedded within a secure label affixed to a paper document or integrated into an ID card-sized carton or polymer card.	A digital identity credential in the form of a VDS, represented as a 2D barcode (QR code), containing a low-resolution photo of the bearer embedded within the QR code and complemented by a high-resolution printed photograph. The embedded chip stores the digital credential, enabling tap-and-go functionality, along with a high-resolution colour photograph.	The chip is securely integrated with the digital credential, ensuring protection against reproduction or duplication. Additionally, the card or paper can be enhanced with traditional security features if necessary.
 Digital ID	No physical document.	The digital credential is stored on the user's mobile phone and can be presented as a 2D barcode (QR code) in the form of a VDS or optionally transmitted via Bluetooth.	The digital credential is secured and bound to the user's device using security measures implemented by the device manufacturer.

Bilateral agreement

The bilateral agreement should establish the legal framework governing key aspects, including the identification of individuals crossing the border, their eligibility and the validity of the associated documentation issued. Following the agreement, both countries will develop the necessary infrastructure to register the identities of individuals within their respective jurisdictions who apply for documentation permitting border crossings under the terms of the agreement.

Identity management

Citizens eligible for the FMZ must be registered and onboarded into the identity management system using valid identity documentation such as passports, birth certificates or other recognized proofs of identity within the country. Alternatively, identity can be established through access to other national identity systems. In all cases, an identity management record is created within each participating country for its citizens under the programme.

If an individual already possesses a national ID card or passport, these documents can be utilized to onboard them into the programme's identity management database. The captured information includes the individual's biographical data in the local language and script, a photograph – either live-captured or sourced from an existing database or identity document – and other biometric details as required. The specific data captured and personalized are determined by the terms of the bilateral agreement between the two countries.

Once an individual's documentation is approved, the respective country issues a border-crossing document containing the citizen's details, country of issuance and the approved validity period. Each country retains control over the approval and eligibility process, ensuring compliance with the policies outlined in the bilateral agreement.

To uphold the integrity of the system, each country must implement measures to verify the accuracy of the information and confirm the individual's identity through biometric verification during the enrolment and onboarding process. This ensures a reliable and secure identity management system for the FMZ.

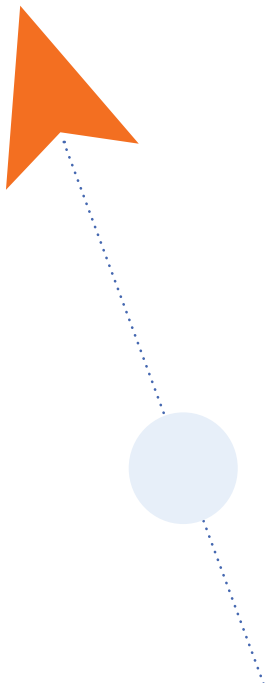
Border control management

The concept of the FMZ, as outlined in the IOM use case, incorporates a streamlined border control process designed to ensure both rapid processing and a sufficient level of security to monitor and manage movement effectively. Given the diverse nature of border control points and their varying infrastructure, the IOM use case accommodates the use of multiple document types. These documents support various verification scenarios and security levels, which are detailed in the subsequent chapters of the IOM Digital ID use case.

The documents issued under the IOM system include paper-based credentials, card or paper-based documents equipped with smart copy protection chips and smart near-field communication (RFID) cards or paper-based labels capable of storing biometric information. This flexibility ensures adaptability to different operational and infrastructure environments.

The system concept is designed to function in rough environments with and without communication connection (offline capability for booking of border crossing and biometric identification). As an option, the system can operate from a normal or industrial-grade personal computer or mobile phone/tablet computer.

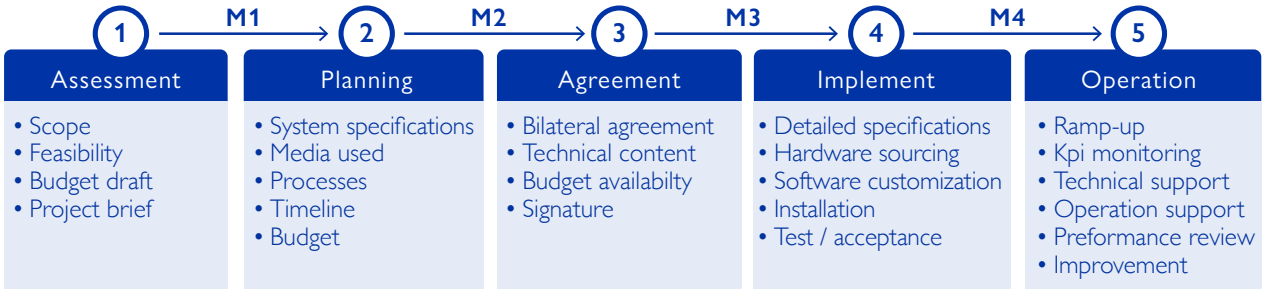
Additionally, the implementation allows for straightforward, simplified and cost-effective Automated Border Control (ABC) gates to facilitate efficient processing while maintaining robust security measures.



3.3 IOM USE CASE IMPLEMENTATION GUIDANCE ON CAPACITY-BUILDING

The implementation of a border-crossing system to support the IOM use case requires an initial bilateral agreement between the participating countries. A critical component of preparing such an agreement is thorough system planning and the definition of detailed use case requirements. This planning process should follow a structured sequence during the analysis phase, culminating in a clear definition of requirements and planned operational flows. The analysis phase includes identifying the necessary data to be collected from eligible individuals, determining the types of passes to be issued and establishing eligibility criteria.

Figure 31. Project implementation flow



3.3.1 ASSESSMENT

The objective of the assessment is to gather comprehensive information regarding the planned implementation of the project, covering all relevant aspects. This assessment includes evaluating the general feasibility of collaboration between the two countries and their ability to establish a bilateral agreement for border crossing using alternative identity documents issued through the IOM system. The assessment examines physical circumstances, available technology, communication infrastructure and the characteristics of the eligible population. Key considerations include the types of individuals involved, their supporting documents and the processes and procedures required for data capture, document issuance and system operation.

Additionally, the assessment should provide an initial budget estimate for the entire project, which is essential for evaluating feasibility and informing decision-making. This budget estimate must encompass overall costs, including implementation and maintenance, as well as specific funding requirements for the next project phase, enabling a realistic and validated financial outlook.

All findings, potential concepts, technological systems and requirements must be documented in a detailed assessment report. Approval of this report concludes the assessment phase, marking the first project milestone (M1). This milestone determines whether the project is feasible, whether sufficient budgets are available and whether it should progress to the detailed planning stage. Following the M1 decision, funds for the planning phase should be allocated to proceed with the next steps.

The assessment should address key areas and summarize findings in an assessment report, providing input for project approval and initial budget allocation. These key areas include:

- **Scope and Geographical Coverage:** Defining the areas and regions involved in the project.
- **Stakeholders and Responsibilities:** Identifying all parties involved and their roles.
- **Technical and Organizational Feasibility:** Outlining the technological and operational requirements for implementation.
- **Budget Allocation:** Estimating planning, implementation, CAPEX and OPEX.
- **Concept Overview and Project Description**: Providing a brief outline of the project's vision and objectives.
- **Identity Policy and Existing Databases:** Assessing the current databases and documents that will form the basis for issuing Digital IDs.
- **Policy and Privacy Considerations:** Addressing data protection, privacy implications for users and agreements between stakeholders.

3.3.2 PLANNING

During the planning phase, all aspects of hardware, software and tokens required for the project are thoroughly evaluated, including includes the necessary digital infrastructure, enrollment facilities, systems and integration requirements. The planning process builds upon the assessment phase to define all details comprehensively. The detailed specifications outline the requirements for operational resources, implementation processes, and Standard Operating Procedures necessary to run the system effectively.

The planning phase results in a detailed technical specification that describes the finalized system design and implementation process. This document should be comprehensive, including timelines, project milestones and a schedule for budget allocation. Detailed cost estimates for implementation, supervision, startup, operational support and ongoing maintenance must also be established. Furthermore, the plan should address all project management resources required to oversee and supervise the implementation on both sides of the partnership.

The planning phase concludes with the approval of technical specifications, project details and budget plans. This marks the second project milestone (M2), during which a main decision is made and final budget availability is confirmed. The content of the planning phase must be tailored to local circumstances and address the following core areas:

Detailed budget plan

- Comprehensive system and technical infrastructure design
- Trust framework agreements among stakeholders
- Technical and financial proposals
- Token budget allocation (e.g. smartcards)
- Costs for project management and supervision
- Implementation costs
- Operation and maintenance budgets
- Licensing and service fees

Project timeline and phases

- Project setup
- Implementation, operational launch and ramp-up
- Optimization phase
- Nominal operation and maintenance

Operation plan

- Standard Operating Procedures
- Maintenance plans
- Training programmes
- User education and information campaigns

Legal and financial requirements

- Bilateral or multilateral agreement obligations
- Legal frameworks and compliance requirements
- Cost-sharing agreements among stakeholders or donors
- Operational controls and financial oversight

3.3.3 AGREEMENT

Once the agreement is established in principle, both countries must negotiate the legal, technical and financial terms of the arrangement. The agreement should comprehensively define all aspects of cross-border movement, including technical system specifications, Digital ID documents and operational procedures. Any involvement from donors or non-governmental organizations to support capacity-building efforts can play a crucial role in facilitating the process.

After finalizing the agreement and defining all legal terms, the document should be formally signed by the designated official representatives. Additionally, the necessary budget allocations must be secured to ensure readiness for implementation.

The following points provide a general framework for the agreement's content. These should be adapted and expanded based on local circumstances and specific requirements:

- Stakeholder responsibilities;
- Technical specifications and contracting principles;
- Token and identity management (acceptance of identities);
- Cost-sharing arrangements between stakeholders for systems and tokens;
- Maintenance and operations organization;
- Security and data exchange;
- Agreement on captured personal data and data privacy for participating citizens of both sides;
- Dispute resolution and investigation process for identity misuse or mismatch.

3.3.4 IMPLEMENTATION

The implementation phase begins with the establishment of the project team and project management structure. A project charter should be created, and project management procedures defined during the project kick-off. Once underway, the project management team should report periodically to a joint project steering committee that oversees progress and ensures alignment with project objectives.

During the final specification phase, all aspects of the solution and associated processes must be thoroughly defined to support procurement, including specifying the types of tokens to be used and the security levels required. The choice of tokens will depend on the available infrastructure and will directly impact the business model and operational costs, including token expenses and any additional associated processes.

The project steering committee, comprising representatives from all stakeholders as outlined in the bilateral agreement, plays a key role in overseeing the implementation phase. This phase concludes once all systems are installed, tested and ready for operation, with trained users and operational infrastructure in place. A dry run is recommended at the end of the testing phase, conducted through a pilot implementation at a single crossing point. This ensures that all functionalities and workflows are operating correctly and provides an opportunity to assess the training of operators and border control personnel.

The implementation phase formally concludes with final acceptance, marking the transition to operational readiness.

Key considerations for the implementation phase:

- Project implementation team and project charter setup;
- Final system specification and definition of operational processes;
- Procurements of systems and software;
- Delivery and installation of systems;
- System functional, capacity testing and compliance / data privacy review;
- Pilot implementation and test on one crossing point;

- Review and adjustment of systems to assure function, data security, privacy and data protection concerns;
- Roll-out to all planned border crossings and enrolment points to an initial setup and gradual expansion during operation if required;
- System acceptance and operational handover planning;
- Administrator and support training implementation;
- Handover of systems to Operation and Maintenance departments.

3.3.5 OPERATION

The operation phase begins gradually with a pilot test conducted during the installation phase. This slight overlap between the implementation and operation phases allows the operations team to gain practical, hands-on experience with the system while providing valuable feedback on functionality and user experience. Incorporating this operational input is essential for reviewing and optimizing the system prior to final acceptance and full operational handover.

As operations start, the initial phase focuses on ramping up activities. During this ramp-up period, it is expected that operational support requirements will be more extensive compared to the subsequent nominal operation phase. Once normal operations are established, the project should continue to receive support, and any necessary improvements should be identified and implemented to ensure sustained efficiency and effectiveness.

Considerations for the Operation phase

- User training
- Maintenance and support process implementation
- Operational Procedures and Operational Manual
- Implementation and operation of KPIs
- Continuous improvement measures such as KPI, compliance and security reviews to ensure the quality of service
- Regular preventive and corrective maintenance, security patching and obsolescence management.

3.4 APPLICATION OF THE DIGITAL IDENTITY TECHNOLOGIES

The application for managing FMZ Digital ID systems is built on the principle of sovereign issuance of digital credentials. This means that each country participating in the FMZ agreement operates its own digital identity management and issuance system independently, under its own jurisdiction. Each country maintains its database of identities, including personal information and entry/exit records, separately. The exchange of information and statistics is conducted according to a protocol established in the bilateral FMZ agreement, which also governs investigative measures for potential fraud or misuse.

Credential verification at FMZ border control points is performed digitally, with minimal manual intervention required for certain types of credentials. Verification can be carried out fully offline on mobile devices such as smartphones or tablets, eliminating dependence on electrical power or communication networks. When installed on a standard personal computer at an FMZ control point or within a basic ABC gate setup, verification remains offline, requiring no communication with external systems. Entry and exit data can be exchanged manually, via mobile devices, through remote connections at a later time, or transported manually. If available, the data can also be transmitted online to a central entry/exit database.

The FMZ use case implements basic Digital ID functionality for issuing Digital ID credentials in the form of a pass. Optionally, the system could include additional functionality, such as a web portal for users to manage their devices, request changes or apply for reissuance of FMZ digital credentials. Features like SSO and transaction approval could also be valuable in this context. The entire system's functionality can be gradually expanded, based on user adoption and demand, to enhance convenience and add value for users.

Issued credentials and trust framework

The credentials issued by participating countries in the FMZ are technically fully compatible but are issued under different trust frameworks. This means the data is digitally signed using the individual keys and PKI infrastructure of the issuing country.

The principal trust framework utilizes the same technology as the signature of travel document credentials, as defined in the ICAO 9303 specification. However, unlike travel document credentials, the PKI information, such as electronic certificates, is managed only bilaterally or multilaterally between the FMZ participating countries. Each country involved in the FMZ agreement operates its own system to sign digital credentials.

The keys and digital certificates used in this context are not linked to or uploaded to the ICAO Public PKD or any other public key directories. Instead, they are created solely for the purpose of issuing FMZ digital credentials.

3.4.1 ENROLLMENT AND ISSUANCE APPLICATION

The enrollment application is responsible for capturing the personal identity information of individuals seeking to obtain a FMZ digital credential. As part of the enrollment process, individuals can present identity documents or other supporting documentation to verify their identity. The type of required documentation and eligibility criteria must be defined and agreed upon by the participating FMZ countries. If a central identity database or other data source is available in the country, it can be connected to retrieve basic identity data.

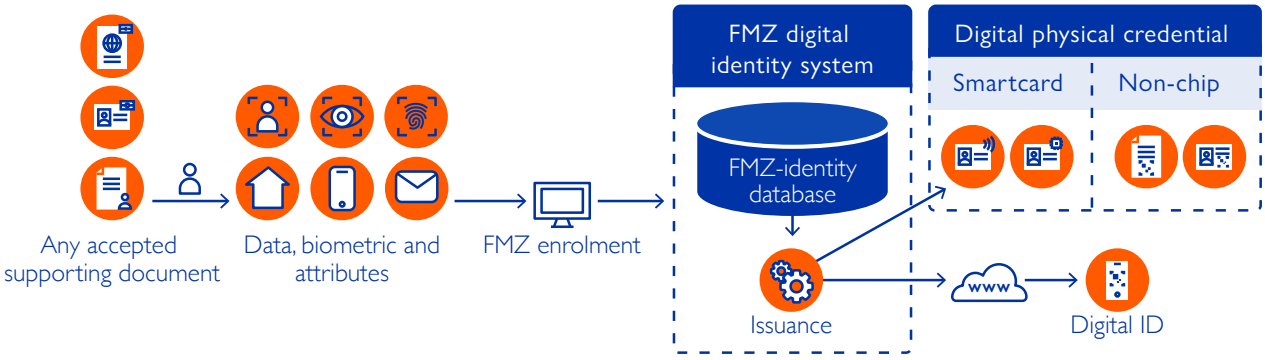
Once an individual's biographic data are enrolled, their biometric data are captured. At a minimum, a photograph must be taken. If a national ID or electronic passport is used as identity proof, the photograph can be electronically extracted from the document. Utilizing pre-existing digitalized information or databases enables a remote issuance process. However, for full data capture, the individual must be physically present during enrollment.

In addition to a photograph, other biometric data such as fingerprints or iris scans, can be captured. The type of biometric data used for verification should be agreed upon as part of the bilateral FMZ agreement. Considering that adding additional biometric data beyond a photograph will increase system costs is important. While a photograph is the most cost-efficient biometric option, it does have limitations. The use of biometric technology should be evaluated based on the required level of identity assurance determined by the participating countries.

During enrollment, other identity attributes are also collected. If a Digital ID on mobile devices is to be used, capturing either an email address or mobile phone number is mandatory, as this information is necessary for the mobile onboarding process.

Once all biometric data are captured, the system verifies the individual's uniqueness and assigns them a UID. This UID must be unique across all participating FMZ countries, ensuring that the individual is identifiable not only within a single country's system but also across the entire FMZ. Including a prefix in the UID, such as the two- or three-letter country code defined in ISO-3166,[26] is advisable.

Figure 32. Digital ID enrolment and issuance system overview



26 ISO, ISO 3166 Country Codes (ISO, n.d.).

3.4.2 DIGITAL CREDENTIAL ISSUANCE

The type of credential used for authentication at FMZ control points must be agreed upon by the participating countries. The credentials issued should align with the geographical and technical circumstances under which the system operates. An important factor to consider is the mode of issuance or re-issuance. Card-based credentials typically require the physical presence of the individual for distribution, while paper-based or Digital ID credentials can often be issued remotely.

All credentials share a principal commonality: the inclusion of a digital credential containing all required information presented as a VDS. This seal is provided in the form of a QR code, which can either be printed on a physical medium or delivered digitally. The VDS includes core information and is digitally signed by the issuing FMZ participating country.

In addition to the VDS, the credential may include a token embedded with an electronic chip. There are two types of chips available. The first is a simple NFC chip with limited data capacity that allows for document origin verification. The second is a smart chip that contains complete identity information and biometric data, enabling full offline biometric verification. These chips can be integrated into an identity card (ID1) format or embedded into a secure label that is applied to paper. Labels are often simpler and more cost-effective than cards, as they can be printed using standard printers, whereas cards require specialized printing devices and maintenance. However, cards provide greater durability and, in the long term, may offer advantages in terms of lifespan and robustness.

Issuing Digital ID credentials is the most cost-effective option once the required infrastructure is in place. However, this method depends on the individual owning a compatible mobile device. The choice between credentials should be based on the specific circumstances at the time of issuance, as well as the verification and security requirements.

As an additional security feature, a biometric template such as a photograph or fingerprint can be embedded within the barcode. This allows for automatic biometric verification even in the absence of a chip. This technology is available and should be assessed for its feasibility based on the specific installation and technical possibilities.

Different credential types provide varying levels of verification at FMZ border control points, offering flexibility to meet the security and operational requirements of the participating countries.

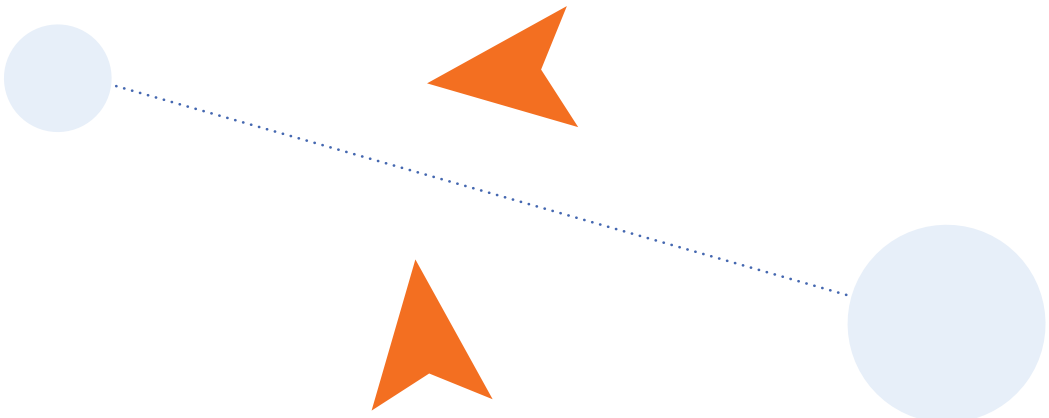
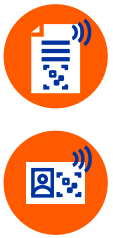
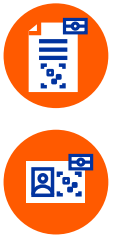


Figure 33. Free Movement Zone Credential Types and Security Levels

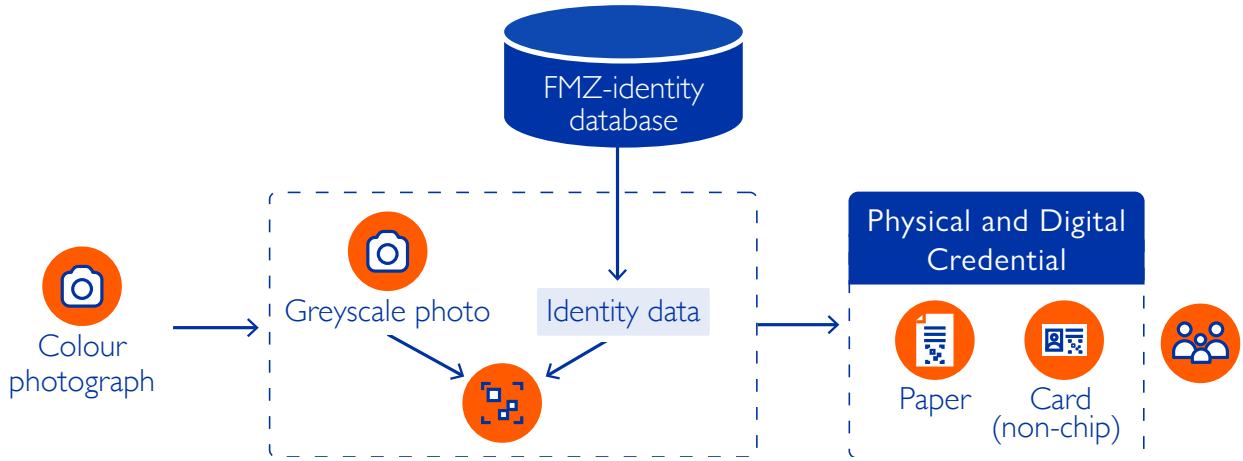
CREDENTIAL TYPE		AUTHENTICITY	CONFIDENTIALITY	ORIGINALITY	BIOMETRIC	COST
	Document or ID Card with QR code VDS (no chip)	HIGH for the data	LOW MEDIUM if encrypted, (static)	LOW Can be copied and requires physical features as protection	MEDIUM with low-resolution photo verification is done manually by border guards HIGH with biometric template in QR code, for automatic check	Low+
	Document Paper / Card and digital credentials 2D barcode with NFC token	HIGH For the data and chip	LOW HIGH if encrypted (dynamic)	HIGH Chip is protecting against copy	MEDIUM with Low-resolution photo) Verification is manually done by border guards HIGH with Biometric Template in QR-Code, for automatic check	Medium
	SmartChip ID or Smart Labels on paper with digital credential in chip and QR code VDS	HIGH For the data and chip	LOW HIGH if encrypted (dynamic)	HIGH Chip is protecting against copy	HIGH with high-resolution photo verification is fully automatic HIGH with biometric template in QR code	Medium+
 Digital-ID	Digital credential and usage as VDS QR code and Bluetooth	HIGH	LOW HIGH if encrypted (dynamic)	LOW HIGH, if mechanism to check the device	HIGH Mainly face biometric	Low

3.4.2.1 NON-CHIP TOKEN WITH VDS

The non-chip token is the simplest and most cost-effective option. It can be issued as a paper document in PDF format, which can be printed remotely, sent by mail or delivered via messaging services. The document includes a high-resolution photograph, either in greyscale or colour, depending on the printer used. It also contains the holder's biographical data, validity and eligibility information and a VDS.

The VDS QR code encodes all the information printed on the paper pass, along with a compressed greyscale photo for verification purposes. The paper token can be used in completely offline environments and verified using a mobile phone or other barcode-reading devices. Additionally, the same data and VDS can be printed on a card in the size of a standard ID card, even without a chip. In card format, the document becomes more durable and easier to handle. However, issuing the card format requires specialized equipment for personalization.

Figure 34. Issuance process of non-chip token with VDS



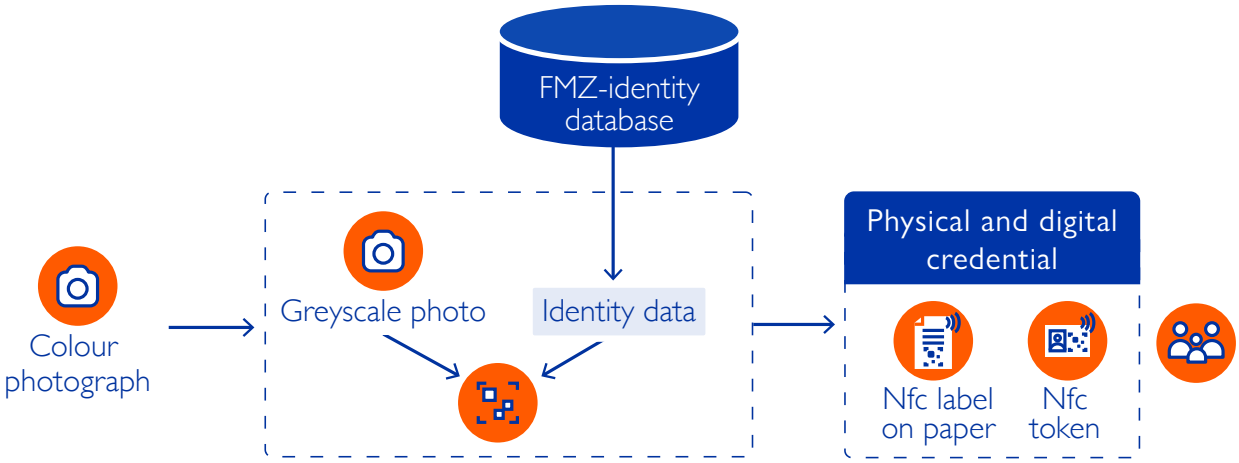
3.4.2.2 NFC TOKEN WITH VDS

The NFC token with a VDS QR code is a chip-based token with an embedded NFC RFID chip. It can be implemented as a smart label or in various ID01 card formats. The chip should comply with a common criteria security level (recommended EAL 3+ or 4) to ensure a sufficient level of security. The NFC token can be integrated into a paper pass with a VDS, providing additional security to the document. The chip enables verification that the holder possesses the original issued document.

To enhance durability compared to a paper-based document with a smart label, the token can also be embedded in a card format and personalized like an ID card. By incorporating the chip into a card, it ensures that the individual has the original card, reducing the risk of copied barcodes being used in the field. The NFC token is further secured with the VDS QR code and supports the same handling and verification methods using a mobile phone or barcode reader.

The NFC token provides a higher level of security compared to a printed VDS on paper alone. Its originality is verifiable through the NFC secure chip, which also serves as a copy-protection mechanism. During verification, both the NFC chip and VDS can be checked, securing the token against copying or counterfeiting. To further protect the token, and when applied as NFC labels, the labels should be physically secured and designed to be destroyed if any attempt is made to remove them.

Figure 35. Issuance process of NFC token with VDS



3.4.2.3 SMARTCHIP TOKEN WITH VDS

The SmartChip token offers higher security and a larger memory capacity, enabling it to store the entire digital credential information. It is recommended to meet a common criteria-evaluated security level of 5 or higher. While ICAO-compliant microprocessor SmartChips could serve as SmartChip tokens, they are typically more expensive than Smart Memory Chips. For the use case presented in this toolkit, Smart Memory Chips are sufficient, as a Common Criteria evaluation level of 5 is considered adequate for government applications.

Smart Memory Chips not only reduce costs but also offer flexibility by enabling embedding into smart labels and various other formats, increasing their usability and adaptability. These chips are widely used in public transportation and other ticketing markets, where low-cost applications and transponders are essential.

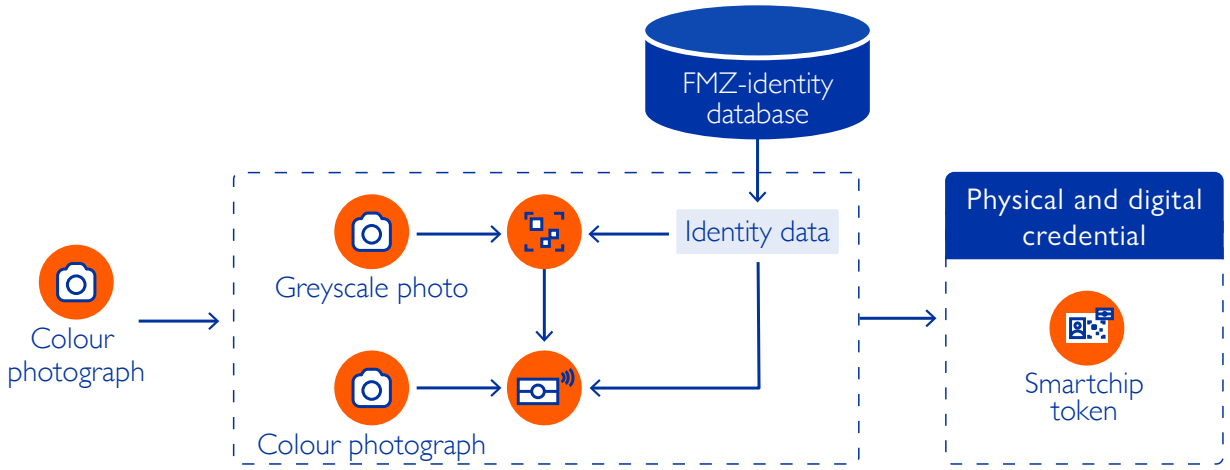
The SmartChip token includes the same VDS as other tokens, with the digital credential printed as a QR code alongside a photograph of the credential holder. Additionally, the digital credential stored in the VDS QR code is also stored in the memory of the SmartChip. The SmartChip features an ISO 7816-compliant file system and supports all relevant security mechanisms for authentication and secure communication. Access to the chip is protected by secret keys that can be customized for each project. Like the trusted framework, key management must be synchronized and organized among the FMZ participating countries.

The ISO file system security mechanism supports different operating modes. In the "tap and go" mode, the data is read-only and protected against alterations. It can be accessed freely, similar to the QR code, or through secured readers where the security keys are stored in a secure module. In the "secured read" mode, users must first present the QR code VDS, which provides information combined with the secure reader's stored key to grant chip access. This mode is similar to the process for passports, where the Machine-Readable Zone must be read before accessing the chip. The choice of mode depends on the decisions of the participating countries. However, the "tap and go" mode offers potentially faster and more efficient processing.

The SmartChip also stores a high-resolution colour photograph of the credential holder, enabling straightforward facial recognition and visualization of the full photo during verification. Like the VDS containing a face biometric template, face recognition can be performed using images, allowing for more generic verification applications, as face templates are often proprietary to specific companies.

Technically, the SmartChip token delivers data similar to that of an ICAO-compliant e-passport but with a lower total cost of ownership.

Figure 36. Issuance process on SmartChip token



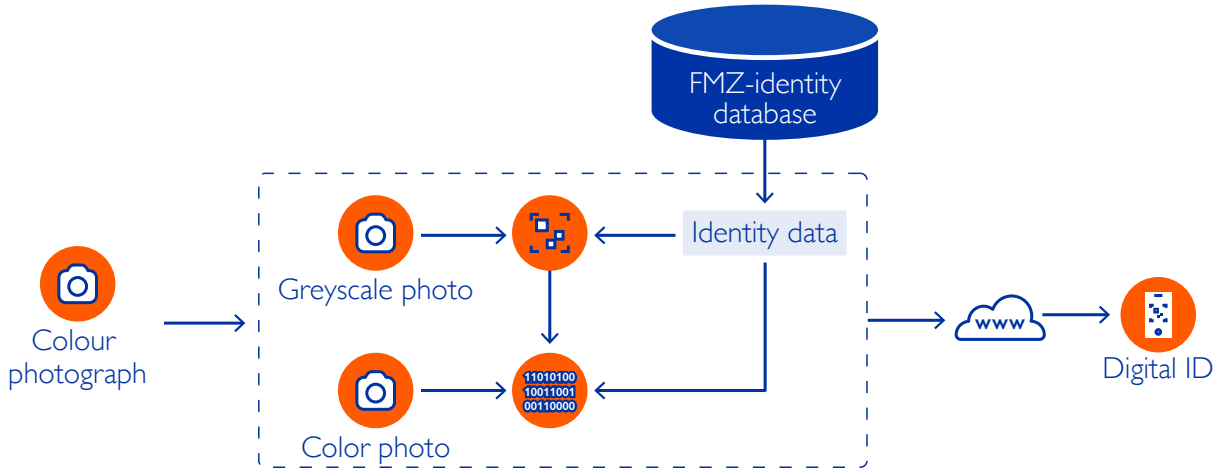
3.4.2.4 DIGITAL ID ON MOBILE DEVICES

To use the Digital ID, the user must have a smartphone and install the Digital ID app on their mobile device. After the user's data are captured in the identity management database during enrollment and they are deemed eligible for FMZ participation, they can proceed to install the FMZ Digital ID. For installation, the user must provide their personal mobile phone number or email address to complete two-factor authentication during the setup process.

Once the Digital ID app is successfully installed, the user can load the digital credential and pass for both offline and online authentication modes. The mobile app includes identity verification through face matching, which is performed during installation and required for each subsequent use. The FMZ pass and authorization can also be managed remotely, allowing for revocation or adjustments to validity based on the user's eligibility.

The mobile device provides more flexible handling of digital credentials, enabling remote management, reissuance and authentication via VDS-QR code and Bluetooth communication with reader terminals.

Figure 37. Digital ID issuance on mobile devices



3.4.3 FMZ ENTRY/EXIT APPLICATION AT THE BORDER

The entry/exist system at the border follows a simple architecture to remain cost-effective. As described in the introduction, it is designed for use in rugged environments and can operate either online or offline, without requiring a constant communication connection.

The system can be built using a standard personal computer or laptop but is also compatible with mobile phones or tablet computers, offering greater flexibility. While a standard ABC gate is technically feasible, its high cost makes it impractical for this use case.

The key components connected to the are:

- **Camera device for photo**

  A device to capture a live photo of the person present at the border point. This could be a standard webcam or an integrated camera in a mobile phone or tablet computer.

- **Camera device for VDS QR code**

  The same webcam or the integrated camera of a mobile phone or tablet computer can also be used to scan the VDS QR code.

- **RFID contactless reader**

  A device for reading chip-based tokens, such as NFC or SmartChip tokens.

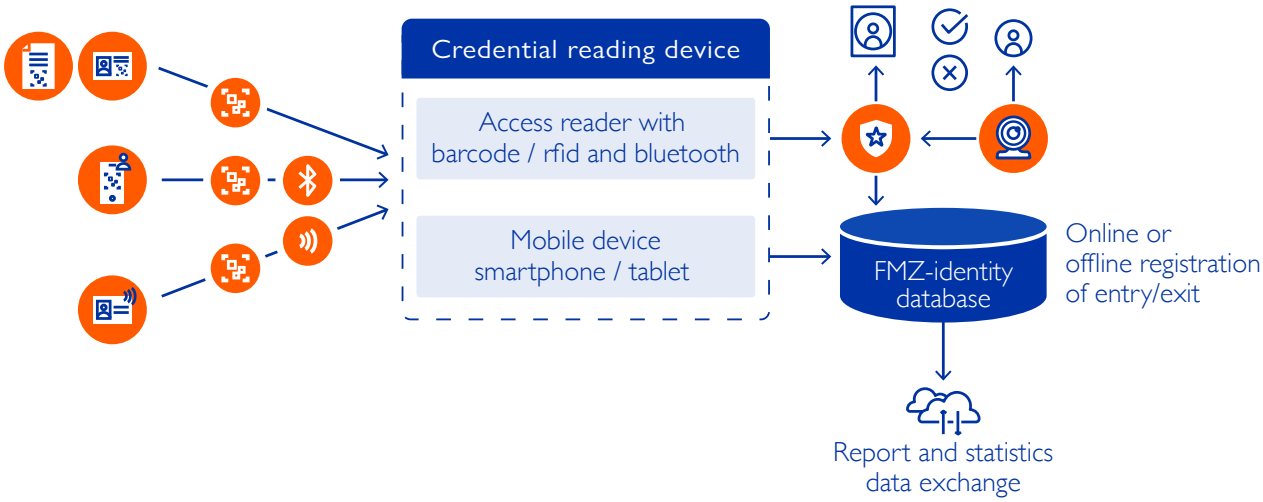
- **Bluetooth reader**

  Used to receive Bluetooth transmissions from the Digital ID app, allowing wireless reading of digital credentials and photographs directly from a smartphone.

Alternatively, combined readers that integrate a QR code scanner, RFID reader and Bluetooth functionality in one device are available. These types of readers, commonly used in access control systems, are cost-effective and easy to handle. A separate combined reader allows ergonomic installation, where the personal computer's webcam remains under the officer's control while the combined reader is positioned conveniently for customer use.

Smartphones and tablet computers typically have all these devices integrated, making them a flexible and cost-effective solution for border control operations.

Figure 38. Entry/exit system overview



Entry and exit transactions can be saved locally and periodically exchanged, either manually or using mobile devices when a mobile data connection is available.

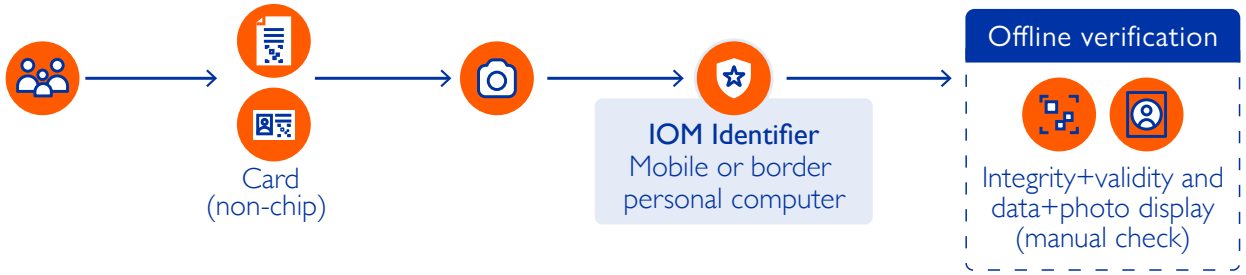
The verification process varies depending on the type of token used, with each method offering a different security level. The selected token type should align with the security requirements of the application. While it is possible to use multiple token types simultaneously within an FMZ system, their security levels and processes differ. This should be taken into account when designing and implementing the system.

3.4.3.1 VERIFICATION SCENARIO – NON-CHIP TOKEN

In the non-chip token scenario, the FMZ user presents only the VDS-QR code, which is typically printed on all FMZ token types. In Figure 28, only standard paper and card tokens without chips are shown; however, the same scenario applies to any token as long as the VDS-QR code is presented.

If all checks are successful, the user is granted passage. If not, the user is directed to a secondary inspection or denied entry.

Figure 39. Verification scenario non-chip token



Handling

The user presents the token with the VDS QR code to the reader.

Process

The VDS QR code is read, decoded and verified:

- Using the digital certificate of the signer to ensure integrity and authenticity (issued by an eligible organization).
- Checking whether the token is valid and not expired.
- Displaying the token information, including the small greyscale photo contained in the token.
- Reading and making the biometric face template available for verification, if the VDS includes one.

Verification

The officer performs the following checks:

- Confirms that the photo in the VDS QR code matches the one printed on the document.
- Ensures that the person presenting the document matches the photo.
- Captures a live photo of the person using a webcam.
- If the token contains a biometric face template, validates the webcam photo against the biometric face template stored in the VDS QR code.

Security

Medium

- The data content is verified.
- The face check is performed manually, but the small greyscale photo in the token provides minimal validation.
- If a biometric face template is stored in the VDS QR code, security is enhanced as an automatic check can be performed.

3.4.3.2 VERIFICATION SCENARIO – NFC TOKEN

Handling

The user presents the token with the VDS QR code to the reader and after the QR code the user presents the token to the RFID reader.

Process

The VDS QR code is read, decoded and verified:

- The verification follows the same steps as for non-chip token.
- Additionally, it is verified that the token is an original token, so the user is in possession of the original. This ensures that no other person can pass the border with a copied VDS QR code.

Verification

The officer performs a check:

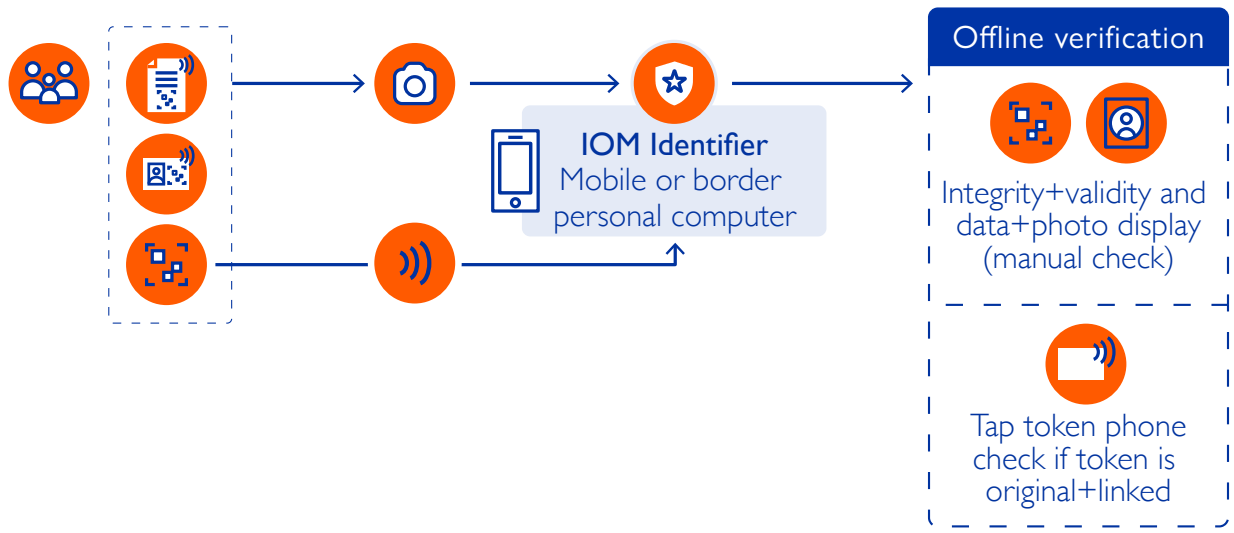
- The same check as with a non-chip token and
- Additionally, the system provides information about whether the chip check was successful.

Security

Medium++

- The data content is verified and the and a manual check performed, same as a non-chip token.
- The chip check confirmed that the user presented the original token (no copy of the VDS QR code).

Figure 40. Verification scenario NFC token



3.4.3.3 VERIFICATION SCENARIO – SMARTCHIP TOKEN

The FMZ Digital ID system must be configured to accommodate different handling options.

Handling

The user has two options:

1. Present the token with the VDS QR code to the reader, followed by presenting the token to the RFID reader.
2. Use the "tap and go" method, where the user only presents the RFID token; the digital credential along with the photo are read directly from the chip.

Process

The VDS QR code is read, decoded and verified:

- The verification process is similar to the NFC token but provides a higher chip security level.
- Additionally, the colour photograph is read from the chip.

Verification

The officer performs the following checks:

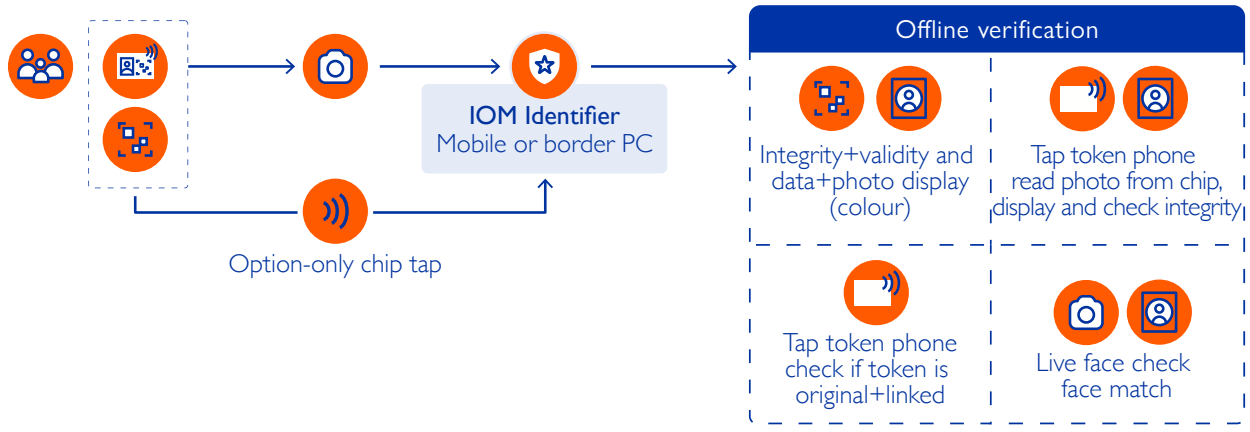
- Similar checks to those conducted with an NFC token.
- Additionally, the system displays a colour photograph of the user for manual and automatic verification. The system supports an ABC gate method at border control points, incorporating a flexible face recognition system. Face recognition using a full photo provides higher accuracy compared to using a face template with only basic characteristics.

Security

High

- Offers similar security to the NFC token but enhanced with a full-colour photo stored on the chip, enabling more robust automatic verification.

Figure 41. Verification scenario SmartChip token



3.4.3.4 VERIFICATION SCENARIO – DIGITAL ID

The FMZ Digital ID system must be configured to support different handling options.

Handling

The user has three options:

1. Present the phone with the VC and VDS QR code to the reader.
2. Use the "tap and go" method, where the phone emulates an RFID token. The digital credential, including the photo, is read directly from the chip.
3. Opt for Bluetooth, where the phone displays a session security code (a random, special QR code). This code is used to establish secure Bluetooth communication between the phone and the reader. After authentication, the digital credential and colour photo are transmitted from the phone to the reader.

Process

The VDS QR code is read, decoded and verified:

- The verification process is similar to that of a SmartChip token.
- Additionally, Bluetooth communication is supported.

Verification

The officer performs the following check:

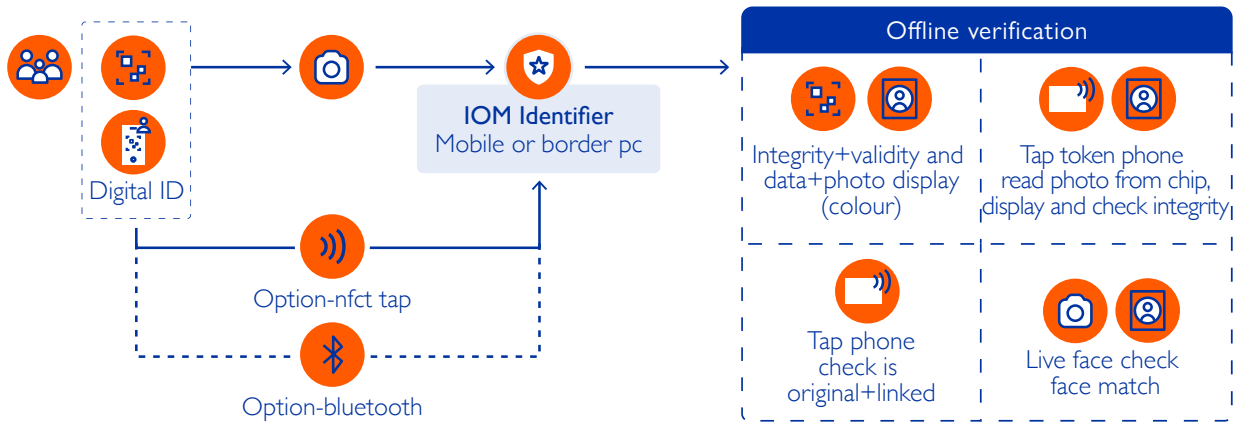
- The verification process is similar to that used with a SmartChip token.

Security

High

- Provides similar security to an NFC token but is enhanced with a full-colour photo stored in the chip, allowing for more robust automatic verification.

Figure 42. Verification scenario of Digital ID



3.5 SUMMARY AND CONCLUSION

The IOM use case for border management in a FMZ using digital credentials and Digital ID represents an implementation of a Digital ID system tailored to a specific user group and project. The principles and technologies described could also be applied to other use cases, as they provide a secure and cost-effective method of identification.

a. The FMZ identity management and Digital ID systems of each participating country operate fully independently.

b. To establish trust, participants exchange only the digital identity signing PKI certificates, enabling secure verification of the digital identity's integrity and origin.

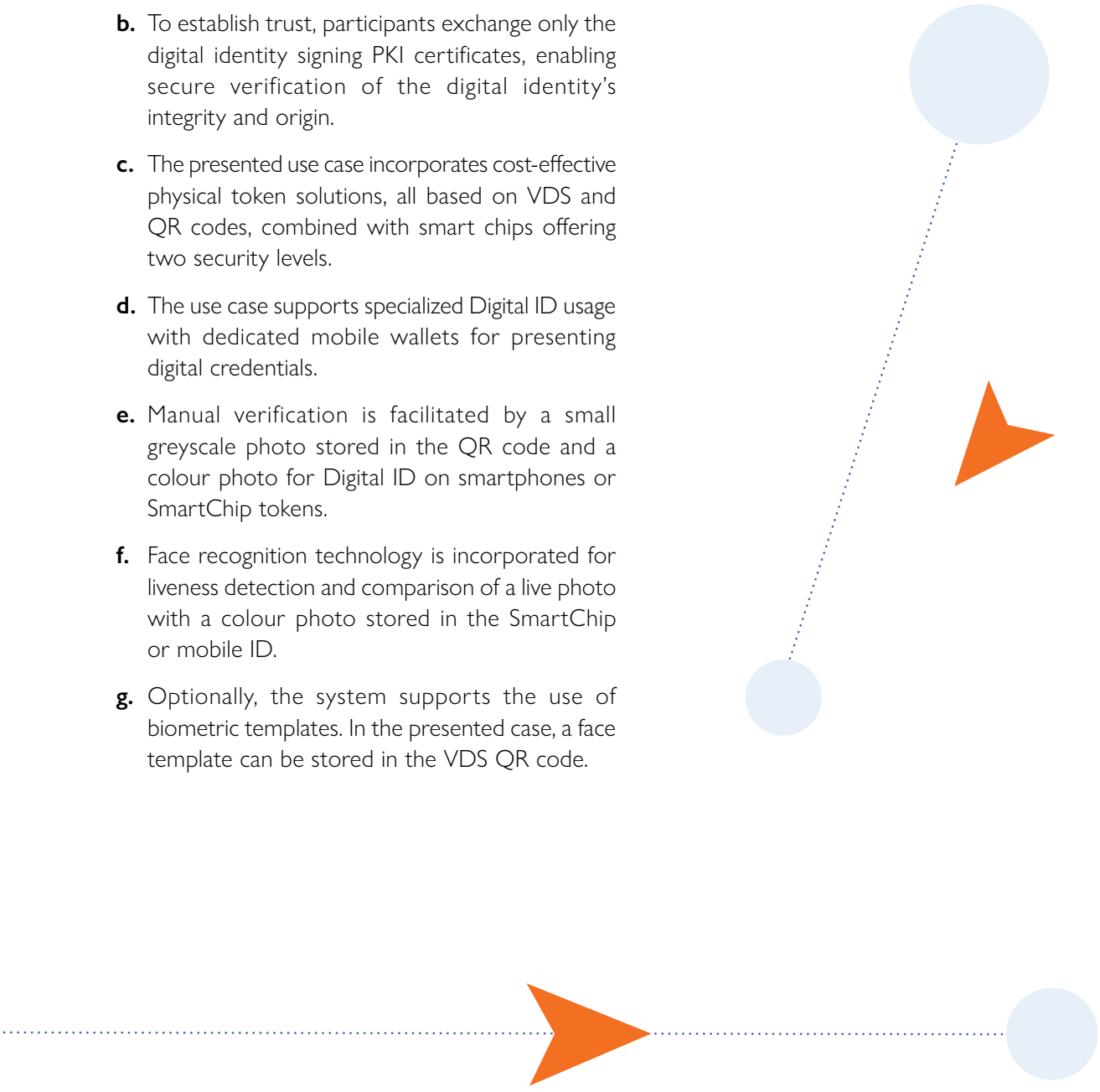
c. The presented use case incorporates cost-effective physical token solutions, all based on VDS and QR codes, combined with smart chips offering two security levels.

d. The use case supports specialized Digital ID usage with dedicated mobile wallets for presenting digital credentials.

e. Manual verification is facilitated by a small greyscale photo stored in the QR code and a colour photo for Digital ID on smartphones or SmartChip tokens.

f. Face recognition technology is incorporated for liveness detection and comparison of a live photo with a colour photo stored in the SmartChip or mobile ID.

g. Optionally, the system supports the use of biometric templates. In the presented case, a face template can be stored in the VDS QR code.



3.6 QUALITY AND SYSTEM PERFORMANCE

To ensure that the system performs as intended and delivers the planned quality and security, a comprehensive set of quality and performance monitoring processes must be established during the implementation phase. These processes should define and continuously monitor KPIs to identify areas for improvement and enhance system efficiency. Tailoring these processes to the specific use case is essential, and all procedures for defining and monitoring KPIs, along with incident response protocols, must be documented in written policies.

A robust monitoring framework should be implemented to track and document daily system usage and performance statistics. Thes data should be summarized in weekly, monthly and quarterly or annual reports to provide a clear view of system ramp-up and nominal operations. These reports will include metrics such as enrolment rates, document issuance and border crossings. Monitoring ensures that workflows are functioning as planned and highlights potential system issues or procedural challenges.

KPIs are divided into quantitative and qualitative categories. Quantitative KPIs measure system statistics and usage trends. These include enrolment rates to monitor how eligible individuals are being onboarded and issued documents, as well as the number of border crossings, which tracks usage patterns and the media types used (for example paper, digital or token-based credentials). Early quantitative indicators reflect ramp-up activities, with stabilization expected during nominal operations. Any deviation from expected values may signal issues requiring immediate attention.

Qualitative KPIs assess system usability and service quality. Objective measures include the time required to complete the enrolment process, accessibility of enrolment locations and processing times at border crossings. These indicators help evaluate the system's ease of use and service quality. Acceptable values for qualitative KPIs should be defined early and adjusted during initial reviews. Once finalized, these values should remain consistent to allow for clear comparisons over time, with corrective actions taken to address any deviations.

Continuous improvement measures should be guided by KPI analysis, ensuring that the system evolves to meet performance expectations. Incidents affecting system functionality or security should trigger a formal incident management process. This process includes an immediate response to mitigate the issue, such as deploying additional staff or increasing controls, followed by a root cause analysis to determine whether the problem is systemic or circumstantial. Corrective actions such as system adjustments, training or procedural changes should be implemented to prevent recurrence. All incidents and responses must be documented in a centralized repository to inform future responses and improve overall system resilience.

The KPI monitoring and incident management procedures should be incorporated into the system's standard operation manual. This document will guide operational teams in managing the system consistently and effectively.

Possible KPIs to monitor the system performance:

a. The number of enrolled eligible FMZ travellers in each participating country, serving as an indicator of system usage, acceptance and the balance of movement.

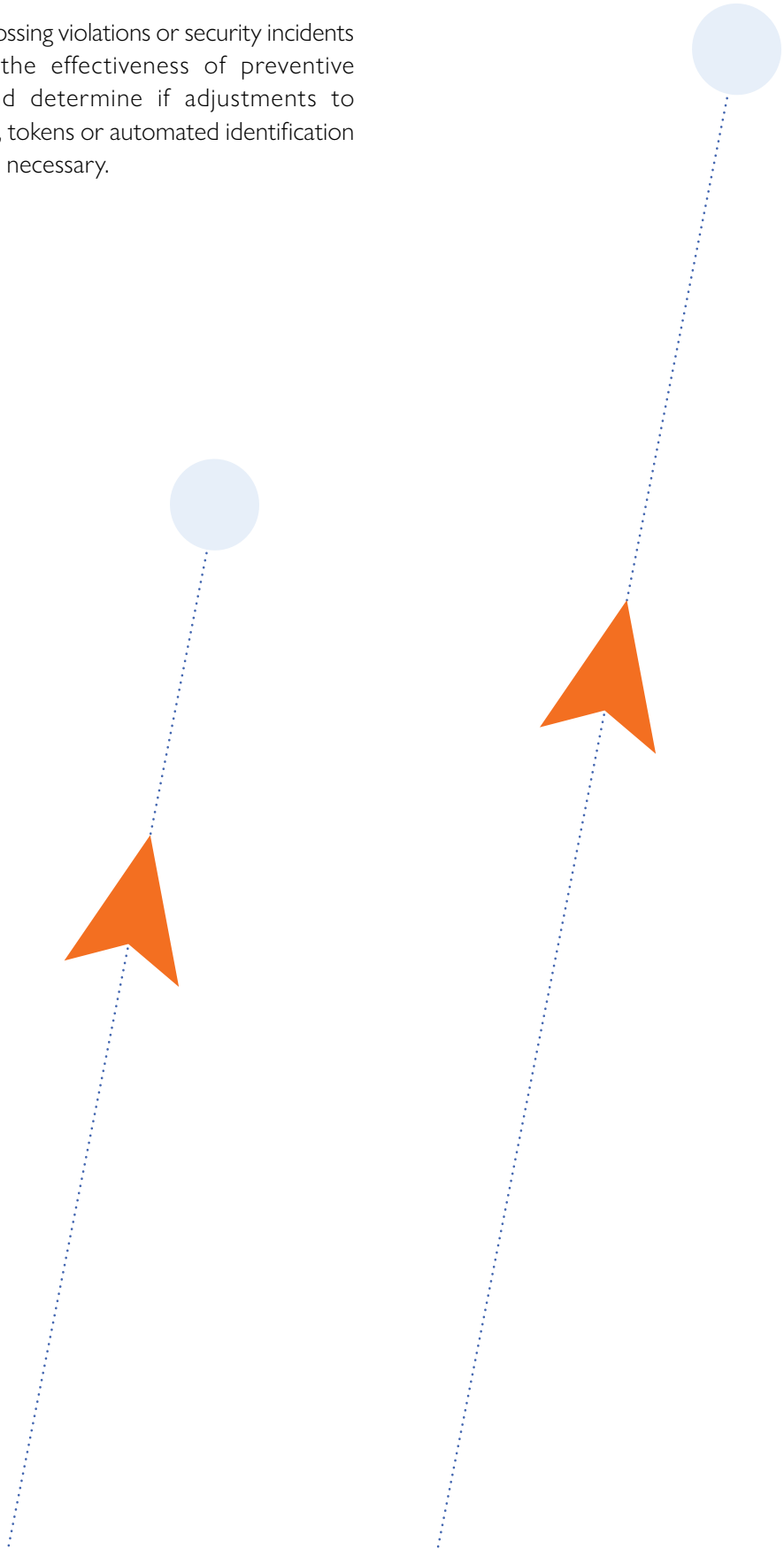
b. The number of travellers and their reasons for participation (such as family, trade, education, visits), providing insights into the socioeconomic impact of the FMZ and guiding corrective measures post-implementation.

c. Measurement of traveller satisfaction through electronic surveys or interviews to identify and address procedural improvements.

d. The number of crossings in each direction at FMZ control points to evaluate flow patterns, overall usage and geographical distribution of movement.

e. Tracking technical malfunctions or system failures to assess availability and ensure the quality of the system.

f. Monitoring crossing violations or security incidents to evaluate the effectiveness of preventive measures and determine if adjustments to security levels, tokens or automated identification processes are necessary.



REFERENCES*

European Union (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Brussels.

Gautam Mitra R., M. Bratschi and G. Mathenge (2021). Population Registers: Definitions and Conceptual Framework. Pacific Community and Vital Strategies, New Caledonia.

Hofstetter, S.D. and R. Rajeshkumar (2021). Free movement zones: guide for issuance and border management. International Organization for Migration, Geneva.

International Civil Aviation Organization (ICAO) (1944). Convention on International Civil Aviation - Doc 7300. Montreal.

ICAO (2016). ICAO Guide: Collection of Best Practices for Acquisition of Machine Readable Travel Documents Goods and Services. Montreal.

ICAO (2018). ICAO TRIP Guide on Evidence of Identity. Montreal.

ICAO (2021). ICAO Doc 9303. Machine Readable Travel Documents. Montreal.

ICAO (n.d.). The ICAO Public Key Directory (PKD). Montreal.

International Organization for Migration (IOM) (2023). Migration Management Digital Maturity Assessment Report - Armenia. Geneva.

International Organization for Standardization (ISO) (2015). ISO 9001:2015 Quality management systems – Requirements. Geneva.

ISO (2015). ISO 14001:2015 Environmental management systems – Requirements with guidance for use. Geneva.

ISO (2018). ISO/IEC 20000-1:2018 Information technology – Service management Part 1: Service management system requirements. Geneva.

ISO (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva.

ISO (2021). ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application. Geneva.

ISO (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva.

ISO (2023). Security and resilience – Authenticity, integrity and trust for products and documents – Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object. Geneva.

* All hyperlinks were working at the time of writing this publication

ISO (2024). ISO/IEC 18004:2024. Information technology – Automatic identification and data capture techniques – QR code bar code symbology specification. Geneva.

ISO (2024). ISO/IEC 16022:2024(en). Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification. Geneva.

ISO (n.d.). ISO 3166 Country Codes. Geneva.

Rajeshkumar R. (2021). Digital Travel Credentials (ICAO, Montreal, TRIP Symposium). 25–28 May.

Sporny M., D. Longley, D. Chadwick and O. Steele (2024). Verifiable Credentials Data Model v2.0. The World Wide Web Consortium.

United Nations (1961). Convention of 5 October 1961 Abolishing the Requirement of Legalization for Foreign Public Documents. The Hague.

United Nations (2014). Principles and Recommendations for a Vital Statistics System. United Nations New York.

United Nations Development Programme and International organization for Migration (2021). Free Movement Zones: Guide for Issuance and Border Management. Geneva.

United Nations Legal Identity Agenda, United Nations Country Team, United Nations Development Programme, United Nations Children's Fund, United Nations DESA, Statistics Division (2020). Operational Guidelines.

United Nations Legal Identity Expert Group (2019). United Nations Strategy for Legal Identity for All. United Nations, New York.

World Bank (n.d.). Brief on digital Identity. Washington, D.C.

www.iom.int
hq@iom.int

17 Route des Morillons
P.O. Box 17, 1211 Geneva 19
Switzerland

@IOMIBG

COMPASS
Guiding safe migration

IOM
UN MIGRATION

Ministry of Foreign Affairs of the Netherlands